
# Local Heights and Densities for Curves of Low Genus

by

**Marco Caselli**

**Thesis**

Submitted to the University of Warwick

for the degree of

**Doctor of Philosophy**

**Department of Mathematics**

September 2018

# Contents

# Acknowledgments

Firstly, I would like to thank my supervisor John Cremona for his guidance, support and constant advice.

I am grateful to the department of Mathematics for the maintenance grant and to the EPSRC for covering my tuition fees.

I would like to thank all the members of the number theory group as well as the PhD students in the maths department, that made my time at Warwick so pleasant. I am grateful to Bill Allombert, Jonas Bergström, Grigoriy Blekherman, Tom Fisher, Everett W. Howe, Marc Masdeu, Christophe Ritzenthaler and Damiano Testa for the stimulating conversations and very useful suggestions.

I am really glad to my great family and the amazing group of friends that have been on my side along the way.

# Declarations

Chapters 1 and 3 are mainly expository and none of the results contained therein are new, whereas some modifications and additions due to the author are present. Part of the computations from Chapter 5 have been discussed by Bergström in [Ber08]. The author was not aware of these counts during the time spent working of the results of Chapter 5. I declare that, unless otherwise indicated and to the best of my knowledge, the contents of this thesis is my own original work. This thesis is submitted to the University of Warwick for the degree of Doctor of Philosophy. No part of this thesis has been submitted towards any other degree.

# Abstract

The thesis consists of two projects, both regarding the localisations of low genus curves.

In the first part we focus on the curves of genus 1. Our aim is to improve the known methods to compute the Canonical Height over an elliptic curve defined over a number field. We show how is not possible to extend directly the method of Bost and Mestre to the complex case. Then, we extend the method of Müller and Stoll for the non-archimedean local height.

The second part is about non-hyperelliptic curves of genus 3. We compute close lower and upper bounds for the density of rational ternary quartics that are everywhere locally solvable by computing the density at each completion of the rationals. In the $p$-adic case we estimate bounds and formulas for the probabilities of solubility of all the possible reductions of a rational ternary quartic defined over $\mathbb{Q}_p$.

# Introduction

This thesis is dedicated to the study of the local heights and densities for curves of low genus. We briefly introduce the content of this work that is organized in two different projects.

## Part I - Computation of the Canonical Height over Number Fields

One of the most important results regarding elliptic curves, defined over a number field $K$, is the Mordell–Weil theorem: it asserts that the group of the $K$-rational points is finitely generated. A very useful tool in the proof of this theorem is the *canonical height*, this function has a key role in finding explicitly the generators of the Mordell–Weil group, but its computation is not straightforward. The most used algorithm nowadays is due to Silverman [Sil88], but when high precision is required timing is deeply affected.

The aim of Part I of this thesis is to find a better and faster way to calculate the canonical height to high precision. Through such an algorithm it would be possible to study numerical examples of the Birch and Swinnerton-Dyer conjecture; moreover it would let us to find linear relations between $K$-rational points, which is used in computing Mordell-Weil groups.

We express the canonical height as sum of local terms and split the computation into archimedean and non-archimedean places, using suitable formulation of the height; then, improving the algorithms for computing the local heights, we obtain an efficient way to compute it.

A key result in the computation of the local height is due to Bernardi, in Chapter 1 we construct the necessary tools to present a detailed proof of it.

In the following statement $K_v$ denotes any completion of the number field $K$, $\lambda_v$ and $\lambda'_v$ denote the local height functions defined below in 1.1.7, while $F_\alpha$ is the kernel polynomial associated to an isogeny $\alpha$, defined in 1.2.5.

**Theorem 1** (Bernardi). *Let $E$ and $E'$ be two elliptic curves defined over $K_v$ and $\alpha : E \to E'$ an isogeny defined over $K_v$ of degree $n$, $\lambda_v$ and $\lambda'_v$ are the local height functions respectively over $E$ and $E'$. Then, for every $P \in E$ not belonging to the kernel of $\alpha$, we have*

$$\lambda'_v(\alpha(P)) = n\lambda_v(P) + v(F_\alpha(P)) + 2v(c_\alpha).$$

The importance of this theorem lies in the capability of keeping track of the local height of a point when we map it to an isogenous curve.

In Chapter 2, this result will let us construct chain of isogenous elliptic curves in order to compute the local height at the archimedean places. In particular, we prove the following Theorem, which is a generalisation of the Bost and Mestre's result from [BM].

**Theorem 2.** *Let $E_0$ be a complex elliptic curve, with equation $E_0 : y^2 = x(x+e)(x+f)$. Then the local height of a point $P_0$ in $E_0 \setminus E_0[2]$ is*

$$\lambda_0(P_0) = \log|z_1| + \sum_{i=1}^{\infty} 2^i \log\left|\frac{z_{i+1}}{z_i}\right| + l,$$

*where $l = \lim_n 2^n\lambda_n(P_n) - 2^n \log|z_n|$ and the $(z_i)_{i\in\mathbb{N}}$ is the sequence defined as $z_i = x_i + a_i^2$: the $x_i$ are the $x$-coordinates of the points in the sequence $(P_i)_{i\in\mathbb{N}}$ and $a_i^2$ are the coefficients from the models of the isogenous elliptic curves defined by the AGM-sequence.*

The limit $l = \lim_n 2^n\lambda_n(P_n) - 2^n \log|z_n|$ is equal to 0 just in the real case but, when we deal with the complex case its behaviour is unknown. Unfortunately this prevents us from describing an extension of the algorithm to the complex case.

For the non-archimedean local height we extend the method introduced by Müller and Stoll in [MS16]. Their algorithm works for rational elliptic curves, here we extend it to any number field $K$.

Gluing together the two methods we have an efficient algorithm to compute the canonical height for elliptic curves defined over totally real number fields.

## Part II - The local solubility of plane quartics

We say that the Hasse principle applies for a certain family of equations when any equation of the family has a rational solution if and only if it has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for each prime $p$. One of the most famous theorems regarding the Hasse principle is the following:

**Theorem 3** (Hasse–Minkowski)**.** *A quadratic form with rational coefficients has a non-trivial zero over $\mathbb{Q}$ if and only if it has a zero over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all primes $p$.*

In the cubic case the Hasse principle fails, and not just for some isolated counterexamples. Indeed, from [Bha14] we have

**Theorem 4** (Bhargava)**.** *A positive proportion of plane cubics fail the Hasse principle.*

This Theorem relies on the probability that a cubic plane curve defined over $\mathbb{Q}$ is everywhere locally solvable, which has been computed by Bhargava, Cremona and Fisher in [BCF15a], providing an exact formula.

The principal aim of Part II is to compute the probability that a non-hyperelliptic curve of genus 3 has a point everywhere locally, extending the work [BCF15a]. As model for those curves we use the ternary plane quartics. Therefore, given a random rational plane quartic, we want to compute the probability that it has points over any completion of $\mathbb{Q}$.

Poonen and Voloch proved in [PV04] that this probability can be computed at each completion of the rationals independently and taking the infinite product of these local probabilities. Knowing this, we separate the computation into real and $p$-adic places.

In Chapter 4 we estimate the density of rational plane quartic having a solution over the reals looking at the cone of positive semi-definite real polynomials. Hilbert's 17th problem gives us a nice characterisation of such polynomials:

**Theorem 5** (Hilbert)**.** *Every definite non-negative real quartic form is the sum of three squares of quadratic forms.*

We then bound the probability of solubility over the reals $\rho(\mathbb{R})$ by

$$0.975068161914319 \leq \rho(\mathbb{R}) \leq 0.9999999684.$$

Moreover, by a Monte Carlo simulation, we estimate the probability over the reals as

$$\rho(\mathbb{R}) \simeq 0.9792.$$

By a different approach, in order to tackle the solubility densities at the non-archimedean completions, in Chapter 5 we classify and count by types of reduction the quartics over $\mathbb{F}_q$. We express these quantities as polynomials in the cardinality of the base field. Thanks to Hensel's Lemma we are able to determine the probability of solubility

for most of the reductions, for the remaining ones we adopt a recursive method which leads to linear relations between these probabilities.

The most difficult cases consist in reduction that are non-reduced curves, which have a number of singular points that is linear in $p$. Indeed, in order to compute the probability of solubility of such curves, we need to compute the correlation between the probabilities of liftability of singular points. In Chapter 6, we analyse the case of conics, computing the probabilities of the number of liftable points. In particular, we notice that the probabilities of lifting two distinct points are not independent.

We then study the probabilities of solubility with respect to the possible reductions of a rational ternary quartic, dividing the computation between the semistable reductions in Chapter 7 and the non-semistable ones in Chapter 8.

Among the possible reductions there are the smooth curves. By the results of W. E. Howe, K. Lauter and J. Top from [HLT05], we know that for $p \geq 31$ all the smooth plane quartics defined over $\mathbb{F}_p$ have at least one point; whereas, for smaller primes, there are examples of pointless smooth curves. From this it follows that we cannot describe by a unique formula the probability of solubility over $\mathbb{Q}_p$ for $p < 31$. Instead, for primes greater than or equal to 31, we have a close estimation of the probability of solubility:

**Theorem 6.** *Let $p$ be a prime greater than or equal to 31, then the probability of solubility over $\mathbb{Q}_p$ of a rational plane quartic is*

$$\rho(\mathbb{Q}_p) = 1 - \frac{1}{2}p^{-4} + \frac{1}{5}p^{-5} - \frac{9}{8}p^{-6} + \frac{41}{24}p^{-7} - \frac{35}{16}p^{-8} + O\left(p^{-9}\right).$$

By this result, computation regarding the real case and bounds for $\rho(\mathbb{Q}_p)$ for small primes we obtain that

**Theorem 7.** *The density $\rho$ of rational plane quartics that are everywhere local soluble satisfies*

$$84.93\% \leq \rho \leq 97.79\%.$$

# Part I

# Algorithms for the canonical height over number fields

# Chapter 1

# Height of elliptic curves over number fields

In this chapter we set the theoretical background needed to formulate the algorithms to compute the canonical height. We will notice that the formal definition of the canonical height is not convenient for computational purposes but, expressing it as sum of local terms, we will be able to compute it efficiently.

We now briefly go through the content of the chapter. Firstly, we describe several equivalent definitions for the canonical height; we define the formulation introduced by Néron, which will be used to compute the archimedean components, and the formulation from Cremona, Prickett and Siksek in [CPS06]. In order to compute the non-archimedean components we describe the setting introduced by Müller and Stoll in [MS16]. The second part of the chapter consists mainly of the proof of the Theorem 1.2.7, stated by Bernardi in [Ber81] where he briefly sketched a proof in few lines. Here we clarify all the details, doing all computations needed and fixing some oversights/mistypes of the original source. This theorem is powerful because it lets us describe the behaviour of the local heights under isogenies, which lead to an iterative method for its computation.

## 1.1 Local heights and isogenies

In this section we state the definitions regarding the height functions attached to an elliptic curve defined over $K$. Throughout this chapter $K$ denotes a fixed number field.

We define the *naive height* for an elliptic curve $E$ as the logarithm of the absolute

height of the $x$-coordinate[1], viewed as an element of the function field $K(E)$. In symbols we can express it as

**Definition 1.1.1.** *The naive height of the point $P \in E(K)$ is*

$$h(P) := \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_k} n_v \log(\max\{1, |x(P)|_v\}),$$

*where $n_v$ is the local degree $[K_v : \mathbb{Q}]$ and $M_K$ denotes the set of normalized absolute values defined over $K$.*

When $K = \mathbb{Q}$, the naive height describes roughly the number of digits we need to express the exact coordinates of the point $P$. It has an "almost" quadratic behaviour. It would be nice to have a function, related to the naive height, that is exactly quadratic. Tate and Néron introduced this tool, called the *canonical height*.

**Definition 1.1.2.** *Let $E$ be an elliptic curve defined over a number field $K$ and $P \in E(K)$, we define the* canonical height[2] *of $P$ as*

$$\hat{h}(P) := \lim_{m \to \infty} \frac{h(2^m P)}{4^m}.$$

The difference between the naive and canonical heights is bounded which makes the canonical height a useful tool to investigate the structure of the rational point over an elliptic curve.

As often happens, gaining interesting properties implies some kind of payback: in this case we have lost the easy computability of the height function. Indeed, the naive height is computable instantly, since it only involves the logarithms of real numbers, in contrast with the canonical height, that is defined by a limit of a sequence that converges slowly and whose terms are computable by recursive polynomials. Therefore, our aim is to reformulate the canonical height in a more computationally suitable way.

We are going to define functions which depends on the models of the elliptic curve $E$; then we recall the definition of the Weierstrass model for $E$ and the associated constants.

[1] This definition could be more general, as in [Sil08, §VIII-6], defining $h(P) := \log(H(f(P)))$, where $f \in \overline{K}(E)$. We preferred to define it with the $x$-coordinate function since this is the most common definition. Moreover, the canonical height, that is the principal topic of this part, is defined independently of this choice.

[2] Silverman here added a factor $1/2$ in the definition to make the canonical height independent of the choice described in the previous footnote 1. The general formula has a factor $1/\deg(f)$. Here we prefer to omit this factor to make the difference between the canonical and naive heights bounded.

**Definition 1.1.3.** *Let $E$ be an elliptic curve given by the Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

*where $a_i \in \mathcal{O}_K$. We set the constants as follows:*

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{aligned}$$

The definition of the canonical height involves the doubling function; we take a closer look at it, introducing the Kummer coordinates to describe it in details.

**Definition 1.1.4.** *Consider the map $\kappa$ from the elliptic curve $E$ to its Kummer variety $E/\{\pm 1\} = \mathbb{P}^1(K)$ defined as*

$$\begin{aligned} \kappa : \quad E &\to \mathbb{P}^1(K) \\ (x : y : 1) &\to (x : 1) \\ O &\to (1 : 0). \end{aligned}$$

*We say that $(x_1, x_2) \in \mathbb{A}^2(K) \setminus \{(0,0)\}$ are a pair of* Kummer coordinates *for $P \in E(K)$ if $\kappa(P) = (x_1 : x_2)$.*

We define two homogeneous polynomials $\delta_1$ and $\delta_2$ as

$$\delta_1(x_1, x_2) = x_1^4 - b_4x_1^2x_2^2 - 2b_6x_1x_2^3 - b_8x_2^4,$$

$$\delta_1(x_1, x_2) = 4x_1^3x_2 + b_2x_1^2x_2^2 + 2b_4x_1x_2^3 + b_6x_2^4,$$

where the $b_i$'s are the coefficients defined in 1.1.3. Then, the doubling function can be read in terms of the Kummer coordinates as described by Müller and Stoll in [MS16], indeed the Kummer coordinates of $2P$ are $\delta(x_1, x_2) := (\delta_1(x_1, x_2), \delta_2(x_1, x_2))$.

Once we have formulated the doubling function in this way, we can similarly reformulate the canonical height using the method in [CPS06]. For every place $v \in M_K$

we define

$$\Phi_v = \frac{\max\{|\delta_1(x_1,x_2)|_v, |\delta_2(x_1,x_2)|_v\}}{\max\{|x_1|_v,|x_2|_v\}^4},$$

which is independent of the choice of the Kummer coordinates of $P$, where the absolute value $|\,|_v$ is normalised in such a way that the archimedean norms, restricted to $\mathbb{Q}$, coincide with the usual absolute value and for the non-archimedean ones we have $|p|_v = p^{-1}$, with $p$ the prime above $v$. From $\Phi_v$, which is continuous and bounded, we define

$$\Psi_v(P) := -\sum_{n=0}^{\infty} 4^{-n-1} \log \Phi_v(2^n P), \tag{1.1}$$

which give us the following reformulation of the canonical height

$$\hat{h}(P) = h(P) - \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \Psi_v(P).$$

Since $h(P)$ is easily computable, the bottle-neck consists in computing the series. To compute the non-archimedean terms we will describe how Müller and Stoll in [MS16] reformulated them in terms of the valuation at the completion of $K$ at $v$, where $v \in M_K$. They defined the function

$$\varepsilon_v(x_1,x_2) := \min\{v(\delta_1(x_1,x_2)), v(\delta_2(x_1,x_2))\} - 4\min\{v(x_1), v(x_2)\},$$

where $v(x) = -\log|x|_v$. The function $\varepsilon_v$ is independent on the choice of the Kummer coordinates of $P$. In the same work they defined the series

$$\mu_v(P) := \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \varepsilon_v(2^n P). \tag{1.2}$$

The reasons to introduce this function are two: if $k$ is the residue field of $K$ at $v$, then we have $n_v \Psi_v(P) = \mu_v(P)\log(\#k)$; moreover we can compute $\mu_v(P)$ exactly just doing a partial sum as proved in [MS16, §IV].

To study the archimedean terms we consider the *local height functions* introduced by Néron.

**Definition 1.1.5.** *The local height function $\lambda_v(P)$ of the point $P$ at the place $v$ is*

$$\lambda_v(P) := \log\max\{1, |x(P)|_v\} - \Psi_v(P),$$

Using these functions we can reformulate the canonical height:

**Theorem 1.1.6** (Néron). *Let $E$ an elliptic curve defined over a number field $K$, then for every point $P \in E(K)\setminus\{O\}$ we have*

$$\hat{h}(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \lambda_v(P).$$

Néron did not construct directly the local heights but defined them by their proprieties:

**Proposition 1.1.7.** *For every place $v \in M_K$ there exists a unique function $\lambda_v : E(K_v)\setminus\{O\} \to \mathbb{R}$, continuous with respect to the $v$-adic topology, such that*

*i) The limit $\lim_{P\to O} \lambda_v(P) + v(x(P)) + \frac{1}{6}v(\Delta)$ exists.*

*ii) For all points $P, Q \in E(K_v)$ such that $P \pm Q \neq O$ we have*

$$\lambda_v(P+Q) + \lambda_v(P-Q) = 2\lambda_v(P) + 2\lambda_v(Q) + 2v(x(P) - x(Q)),$$

*where $\Delta$ is the discriminant of $E$.*

*These $\lambda_v$ are called* local height functions.

The $\lambda_v$ are quasi-quadratic functions, indeed the second property in the above proposition is equivalent to

$$\lambda_v(2P) = 4\lambda_v(P) + 2v(2y(P)),$$

for every $P \in E(K_v)$ such that $2P \neq O$.

The details and proofs of the preceding arguments can be found in [Sil99, §VI]; notice that the normalisation in the reference does not coincide with the one we are currently using.

## 1.2 The relation between local heights and isogenies

This section is dedicated to the statement and proof of Bernardi's Theorem 1.2.7. We split the content of the proof into some remarks and propositions with two aims: to make the exposition easier to be understood and to present clearly some general results (whose relevance is independent from the theorem) such as the one shown in 1.2.3.

Now we define and study an invariant associated to isogenies between elliptic curves.

**Definition 1.2.1.** *Let $(E,\omega)$ and $(E',\omega')$ be two elliptic curves over a field $K$ with respectively invariant differentials $\omega$ and $\omega'$, let $\alpha : E \to E'$ be an isogeny. We associate an invariant to the isogeny as follows. The isogeny induces a map between the spaces of differential forms over the two elliptic curves*

$$\begin{aligned}\alpha^* :&\Omega_{E'} \to \Omega_E\\ &\omega' \mapsto c_\alpha \cdot \omega\end{aligned}$$

*where $c_\alpha \in K$ and is not null if and only if $\alpha$ is separable.*

*A standard choice of the invariant differential $\omega_E$, that is the $K$-generator of the space of differential forms $\Omega_E$, is*

$$\omega_E = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}$$

*where $E$ is in the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.*

*Moreover, the isogeny $\alpha$ is said to be normalised if $c_\alpha = 1$.*

*Remark* 1.2.2. In the case $K = \mathbb{C}$ the constant $c_\alpha$ has a further interpretation. Indeed, recalling that there is an isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$, every isogeny $E \to E'$ is induced by multiplication by some $c \in \mathbb{C}^*$, see [Sil08, §VI-5.3]. On $\mathbb{C}/\Lambda$ the invariant differential is simply $dz$. The situation may be illustrated as follows:

$$\begin{array}{ccc} E & \xrightarrow{\alpha} & E' \\ \| & & \| \\ \mathbb{C}/\Lambda & \longrightarrow & \mathbb{C}/\Lambda' \\ z_\Lambda & \longmapsto & c_\alpha z_\Lambda = z_{\Lambda'}. \end{array}$$

Since $\alpha^*$ is computed by differentiating $\alpha$, we have

$$\alpha^*(dz_{\Lambda'}) = c_\alpha dz_\Lambda.$$

Here we describe two useful formulas related to the invariant $c_\alpha$.

**Lemma 1.2.3.** *Let $E$ and $E'$ be elliptic curves defined by Weierstrass equations over a complete field $K$. Let $\alpha$ be a separable isogeny between $E$ and $E'$, then we have*

$$\lim_{P\to O}\frac{x_{E'}(\alpha(P))}{x_E(P)} = c_\alpha^{-2}$$

$$\lim_{P\to O}\frac{y_{E'}(\alpha(P))}{y_E(P)} = c_\alpha^{-3}.$$

*Proof.* The theorem is true in every field but when $\mathrm{char}(K) = 2$ the computations are a bit more involved, therefore we will split the proof in two cases. Let us first assume that the characteristic of $K$ is not 2. We pick a model of $E$ such that its Weierstrass equation is medium, i.e. $a_1 = a_3 = 0$.

Let $P = (x_E, y_E)$ be a point in $E(K)$; in [Was08, §2.9] it is shown that its image is

$$\alpha(P) = \alpha(x_E, y_E) = (r(x_E), y_E \cdot s(x_E)) =: (x_{E'}, y_{E'}),$$

where $r(x_E)$ and $s(x_E)$ are rational functions. Noticing that

$$c_\alpha\frac{dx_E}{2y_E} = \alpha^*\left(\frac{dx_{E'}}{2y_{E'}}\right) = \frac{r'(x_E)dx_E}{s(x_E)2y_E}$$

we have another expression of the image of a point

$$\alpha\big((x_E, y_E)\big) = (r(x_E), y_E c_\alpha^{-1} r'(x_E)).$$

Therefore, we have

$$\lim_{P\to O}\frac{y_{E'}}{y_E} = c_\alpha^{-1}\lim_{P\to O} r'(x_E) = c_\alpha^{-1}\lim_{P\to O}\frac{r(x_E)}{x_E} = c_\alpha^{-1}\lim_{P\to O}\frac{x_{E'}}{x_E}$$

where the equality in the middle holds by L'Hôpital's rule. Moreover, we know that

$$\lim_{P\to O}\left(\frac{y_{E'}}{y_E}\right)^2 = \lim_{P\to O}\frac{x_{E'}^3 + a'x_{E'} + b'}{x_E^3 + ax_E + b} = \lim_{P\to O}\left(\frac{x_{E'}}{x_E}\right)^3$$

which implies

$$\lim_{P\to O}\left(\frac{x_{E'}}{x_E}\right)^3 = \lim_{P\to O}\left(\frac{y_{E'}}{y_E}\right)^2 = c_\alpha^{-2}\lim_{P\to O}\left(\frac{x_{E'}}{x_E}\right)^2$$

and we conclude that

$$\lim_{P\to O}\frac{x_{E'}}{x_E} = c_\alpha^{-2}$$

and

$$\lim_{P\to O}\frac{y_{E'}}{y_E}=c_\alpha^{-3}.$$

Now let us consider the case when the characteristic of $K$ is 2. First of all we need to work out how to describe the coordinates of the image of a point $P=(x_E,y_E)$.

Every element $R(x,y)\in\bar{K}(E)$ has the form $r(x)+ys(x)$, with $r,s\in\bar{K}(x)$.

Therefore $\alpha:E(\bar{K})\to E'(\bar{K})$ can be described as

$$\alpha((x,y))=(r_1(x)+ys_1(x),r_2(x)+ys_2(x)).$$

The equality $\alpha(-P)=-\alpha(P)$ implies

$$\begin{cases}(a_1x+a_3)s_1(x)=0\\(a_1x+a_3)s_2(x)+a_1'r_1(x)+ya_1's_1(x)+a_3'=0\end{cases}$$

and, since $(a_1,a_3)\neq(0,0)$ because $E$ is non-singular, we have

$$s_1(x)=0,\qquad (a_1x+a_3)s_2(x)=a_1'r_1(x)+a_3'.$$

Then we can compute $c_\alpha$, indeed

$$\begin{aligned}c_\alpha\cdot\frac{dx_E}{(a_1x_E+a_3)}=\alpha^*\left(\frac{dx_{E'}}{(a_1'x_{E'}+a_3')}\right)&=\frac{r_1'(x)dx_E}{(a_1r_1(x)+a_3')}\\&=\frac{r_1'(x)dx_E}{(a_1x_E+a_3)s_2(x)}=\frac{r_1'(x)}{s_2(x)}\cdot\frac{dx_E}{a_1x_E+a_3}.\end{aligned}$$

Therefore $s_2(x)=c_\alpha^{-1}r_1'(x)$ and then we have

$$\alpha((x,y))=(r_1(x),r_2(x)+yc_\alpha^{-1}r_1'(x)).$$

Now it is just a matter of applying a method similar to the one in the previous case.

$$\begin{aligned}\lim_{P\to O}\frac{y_{E'}}{y_E} &= \lim_{P\to O}\frac{r_2(x)}{y} + c_\alpha^{-1}\lim_{P\to O} r'(x_E)\\ &= \lim_{P\to O}\frac{r_2(x)}{y} + c_\alpha^{-1}\lim_{P\to O}\frac{r(x_E)}{x_E} \qquad \text{(L'Hôpital's rule)}\\ &= \lim_{P\to O}\frac{r_2(x)}{y} + c_\alpha^{-1}\lim_{P\to O}\frac{x_{E'}}{x_E}.\end{aligned}$$

Moreover, we know that

$$\lim_{P\to O}\left(\frac{y_{E'}}{y_E}\right)^2 = \lim_{P\to O}\frac{a_1'x_{E'}y_{E'} + a_3'y_{E'} + x_{E'}^3 + a_2'x_{E'}^2 + a_4'x_{E'} + a_6'}{a_1x_Ey_E + a_3y_E + x_E^3 + a_2x_E^2 + a_4x_E + a_6} = \lim_{P\to O}\left(\frac{x_{E'}}{x_E}\right)^3$$

because the orders at the infinity point $O$ of $x_E$ and $x_{E'}$ are equal to 2.

We can conclude, using the same equality as in the previous case, if $\lim_{P\to O}\frac{r_2(x)}{y} = 0$. Notice that $y_{E'} = r_2(x) + yc_\alpha^{-1}r_1'(x)$ has a pole of order 3 at $O$. Therefore $r_2(x)$ has at most a pole of order 3 at $O$ and, since is a polynomial in $x_E$, has even order, so $r_2(x)$ has order at most 2. Since $y_E$ has a pole of order 3 we conclude. □

From the proof above follows this equality that will be useful further on.

**Corollary 1.2.4.** *Let $\alpha : E \to E'$ be an isogeny described by $\alpha(P) = (r(x_E), y_E \cdot s(x_E))$, then*

$$c_\alpha = \frac{r'(x_E)}{s(x_E)}.$$

We next introduce a rational function over $E$ associated to the isogeny $\alpha$.

**Definition 1.2.5.** *We define the* kernel polynomial of $\alpha$ *as*

$$F_\alpha(P) := \prod_{\substack{T\in\ker\alpha,\\ T\neq 0}} \big(x - x(T)\big) \in K[x].$$

The following is a technical lemma useful to prove the Theorem 1.2.7.

**Lemma 1.2.6.** *Let $n$ be the degree of the isogeny $\alpha$. The rational function $g_\alpha$ defined over $E \times E$ as*

$$g_\alpha(P,Q) = \frac{\big(x(\alpha(P)) - x(\alpha(Q))\big)^2}{(x(P) - x(Q))^{2n}} \cdot \frac{F_\alpha^2(P)F_\alpha^2(Q)}{F_\alpha(P+Q)F_\alpha(P-Q)}$$

*is constant and equal to $c_\alpha^{-4}$.*

*Proof.* In order to show that $g_\alpha$ is constant we will compute its divisor. First of all we fix a point $\bar{P}$, not belonging to $\ker\alpha$, and we compute the divisor of $g_\alpha(\bar{P},Q)$, that is a rational function over $E$. Since $g_\alpha(\bar{P},Q)$ is a product of several functions we compute the divisor separately for each factor. We recall that the function $x$ has a pole of multiplicity 2 at the infinity point $O$.

Let us start counting the zeros of $x(\alpha(\bar{P}))-x(\alpha(Q))$:

$$\begin{aligned} x(\alpha(\bar{P}))-x(\alpha(Q))=0 &\iff x(\alpha(\bar{P}))=x(\alpha(Q)) \iff \pm\alpha(\bar{P})=\alpha(Q)\\ &\iff \alpha(\pm\bar{P}-Q)=O \iff \pm\bar{P}-Q\in\ker\alpha\\ &\iff Q=T\pm\bar{P},\ T\in\ker\alpha. \end{aligned}$$

It has poles of order 2 when $\alpha(Q)=O \iff Q\in\ker\alpha$, so

$$\operatorname{div}(x(\alpha(\bar{P}))-x(\alpha(Q)))=\sum_{T\in\ker\alpha}([T+\bar{P}]+[T-\bar{P}])-2\sum_{T\in\ker\alpha}[T].$$

The zeros of $x(\bar{P})-x(Q)$ are just $\pm\bar{P}$, so

$$\operatorname{div}(x(\bar{P})-x(Q))=[\bar{P}]+[-\bar{P}]-2[O].$$

Let us look at the factors involving $F_\alpha$. $F_\alpha(\bar{P})$ is constant hence its divisor is 0. Then

$$\begin{aligned} F_\alpha(Q)=0 &\iff x(Q)=x(T) \text{ for some } T\in\ker\alpha\\ &\iff Q=\pm T, \text{ for some } T\in\ker\alpha \end{aligned}$$

and when $Q=O$ each of the $n-1$ terms has a pole of order 2 so

$$\operatorname{div}(F_\alpha(Q))=2\sum_{\substack{T\in\ker\alpha,\\ T\neq O}}[T]-2(n-1)[O].$$

The above argument works also if $T=-T$ for some $T\in\ker\alpha$, indeed in this case $x(P)-x(T)$ has a zero of order 2 in $T$. One can compute the last two divisors using [Sil08, §II-3.6] with $\phi$ the translation by $\bar{P}$ (in the latter case also a reflection is needed) and obtain

$$\operatorname{div}(F_\alpha(\bar{P}+Q)) = 2\sum_{\substack{T\in\ker\alpha,\\ T\neq O}}[T-\bar{P}] - 2(n-1)[O],$$

$$\operatorname{div}(F_\alpha(\bar{P}-Q)) = 2\sum_{\substack{T\in\ker\alpha,\\ T\neq O}}[T+\bar{P}] - 2(n-1)[O].$$

Adding each divisor with the proper coefficients we obtain

$$\operatorname{div}(g_\alpha(\bar{P},Q)) = 0.$$

Therefore $g_\alpha(\bar{P},Q)$ is a constant for every choice of $\bar{P}\notin\ker\alpha$, but not necessarily the same constant. Notice that $g_\alpha(P,Q)=g_\alpha(Q,P)$ for all $P,Q\in E$, then also $g_\alpha(Q,\bar{P})$ is constant and therefore we get that $g_\alpha(P,Q)$ is constant if either $P$ or $Q$ are not in $\ker\alpha$. Hence $g_\alpha(P,Q)$ is constant over $E\times E$ except on possibly a finite set; but then it is constant everywhere, since it is a rational function.

In order to show that this constant value is $c_\alpha^{-4}$ we can compute it at any $(P,Q)\in E\times E$. In particular we fix, as before, a point $\bar{P}$ not belonging to $\ker\alpha$ and we let $Q\to O$. We rearrange $g_\alpha$ as a product of 3 factors

$$g_\alpha(P,Q) = \frac{(x(\alpha(P))-x(\alpha(Q))^2}{(x(P)-x(Q))^2}\cdot\frac{F_\alpha^2(P)}{F_\alpha(P+Q)F_\alpha(P-Q)}\cdot\frac{F_\alpha^2(Q)}{(x(P)-x(Q))^{2n-2}}.$$

Then we compute the limits of each factor

$$\lim_{Q\to O}\frac{(x(\alpha(\bar{P}))-x(\alpha(Q))^2}{\big(x(\bar{P})-x(Q)\big)^2} = \lim_{Q\to O}\left(\frac{x(\alpha(Q))}{x(Q)}\right)^2 \overset{1.2.3}{=} c_\alpha^{-4}$$

$$\lim_{Q\to O}\frac{F_\alpha^2(\bar{P})}{F_\alpha(\bar{P}+Q)F_\alpha(\bar{P}-Q)} = \frac{F_\alpha^2(\bar{P})}{F_\alpha(\bar{P})F_\alpha(\bar{P})} = 1$$

$$\lim_{Q\to O}\frac{F_\alpha^2(Q)}{(x(\bar{P})-x(Q))^{2n-2}} = \lim_{Q\to O}\prod_{\substack{T\in\ker\alpha,\\ T\neq O}}\frac{(x(Q)-x(T))^2}{(x(\bar{P})-x(Q))^2} = 1.$$

Since these limits are finite we conclude

$$g_\alpha(P,Q) = \lim_{Q\to O} g_\alpha(\bar{P},Q) = c_\alpha^{-4}.$$

□

Finally, we have enough tools and results to prove Bernardi's theorem as stated in [Ber81].

**Theorem 1.2.7** (Bernardi). *Let $E$ and $E'$ be two elliptic curves defined over $K_v$ and $\alpha : E \to E'$ an isogeny defined over $K_v$ of degree $n$, $\lambda_v$ and $\lambda'_v$ are the functions respectively over $E$ and $E'$ described in Proposition 1.1.7. Then, for every $P \in E$ not belonging to the kernel of $\alpha$, we have*[3]

$$\lambda'_v(\alpha(P)) = n\lambda_v(P) + v(F_\alpha(P)) + 2v(c_\alpha).$$

*Proof.* The equation in the statement has a part dependent on $P$ and the rest is constant, so actually we want to prove that

$$f(P) = \lambda'_v(\alpha(P)) - n\lambda_v(P) - v(F_\alpha(P))$$

is constant and equal to $2v(c_\alpha)$. We cannot evaluate $\lambda_v$ but we can somehow cancel it out using (1.1.7.ii), indeed computing the remainder $r(P,Q)$ of the parallelogram law we have

$$\begin{aligned} r(P,Q) &= f(P+Q) + f(P-Q) - 2f(P) - 2f(Q) \\ &= v\left(\frac{(x(\alpha(P)) - x(\alpha(Q))^2}{(x(P)-x(Q))^{2n}} \cdot \frac{F_\alpha^2(P)F_\alpha^2(Q)}{F_\alpha(P+Q)F_\alpha(P-Q)}\right) \\ &\overset{1.2.6}{=} v\left(g_\alpha(P,Q)\right) \overset{1.2.6}{=} v\left(c_\alpha^{-4}\right) = -4v\left(c_\alpha\right). \end{aligned}$$

Since $f$ is continuous, if we prove that the limit of $f(P)$ exists when $P$ tends to a point in the kernel, we can extend $f$ by continuity to $\bar{f}$ preserving the remainder of the parallelogram law. Hence, if $O \neq T \in \ker\alpha$,

$$\begin{aligned} \lim_{P\to T} f(P) &= \lim_{P\to T} \lambda'_v(\alpha(P)) - n\lambda_v(T) - v(F_\alpha(P)) \\ &\overset{1.1.7}{=} \lim_{P\to T} -v(x(\alpha(P))) - v((x(P)-x(T))(x(P)-x(-T)) + k \\ &= \lim_{P\to T} -v\Big(x(\alpha(P))(x(P)-x(T))(x(P)-x(-T))\Big) + k \end{aligned}$$

[3] This result was stated by Bernardi in [Ber81], using a different normalisation for $\lambda_v$, in terms of the value $\lim_{P\to O} \frac{x_{E'}(\alpha(P))}{x_E(P)}$. Here we preferred to state the formula using the invariant $c_\alpha$ associated to the isogeny.

where $k$ is a constant independent of $P$. The last expression is a finite value since $x(\alpha(P))$ has a pole of order 2 in $T$ and $(x(P)-x(T))(x(P)-x(-T))$ has a zero of order 2 in $T$. This argument works also if $2T = O$, indeed in this case $x(P)-x(T)$ has a zero of order 2 in $T$. On the other hand, if $T = O$, we have

$$\begin{aligned}\lim_{P\to O} f(P) &= \lim_{P\to O} \lambda'_v(\alpha(P)) - n\lambda_v(P) - v(F_\alpha(P)) \\ &\overset{1.1.7}{=} \lim_{P\to O} -v(x(\alpha(P))) + nv(x(P)) - v(F_\alpha(P)) + k' \\ &= \lim_{P\to O} v\left(\frac{x(P)^{n-1}}{F_\alpha(P)} \cdot \frac{x(P)}{x(\alpha(P))}\right) + k' \\ &\overset{1.2.3}{=} \lim_{P\to O} v\left(c_\alpha^{-2}\right) + k'.\end{aligned}$$

where $k'$ is a constant value independent of $P$.

Consider now $\tilde{f} := \bar{f} + 2v\,(c_\alpha)$, this function satisfies the parallelogram law, i.e. is quadratic, that means

$$\tilde{f}(mP) = m^2\tilde{f}(P).$$

Remembering that $\bar{f}$ is continuous with respect to the $v$-adic topology also $\tilde{f}$ is continuous. By Weierstrass theorem for continuous functions over a compact space (that in our case is $E(K_v)$), $\tilde{f}(E)$ is bounded, but since it is quadratic we have that $\tilde{f} = 0$, and then

$$f(P) = 2v(c_\alpha).$$

□

This result lets us move from one elliptic curve to another keeping track of the heights of the points. In particular, we notice that a translation does not influence the local heights, i.e. $\lambda_E$ is independent of the model of the elliptic curve $E$. By coordinate translation we mean an isomorphism $\alpha$ between Weierstrass models of elliptic curves $E$ and $E'$ described by $(x, y) \mapsto (x + r, y + t)$.

**Corollary 1.2.8.** *If $\alpha$ is an isomorphism the local and canonical heights are preserved. In particular, the local and canonical height are preserved by coordinates translation.*

*Proof.* Since $\alpha$ is an isomorphism its degree is $n = 1$ and its kernel is just the origin $O$, it follows that $F_\alpha = 1$. Moreover $c_\alpha = 1$. Putting everything in the formula of the Theorem 1.2.7 we have

$$\lambda'_v(\alpha(P)) = \lambda_v(P) + v(1) + 2v(1) = \lambda_v(P).$$

Notice that this also implies the canonical height, which is sum of local heights, is preserved by isomorphism between models.

Since the coordinate translation is an isomorphism between Weierstrass models of elliptic curves $E$ and $E'$ we conclude. $\square$

# Chapter 2

# Computation of the local heights

We apply the results from Chapter 1 to compute the local archimedean height. Bost and Mestre in the notes [BM] described a method for real elliptic curves, involving chains of isogenous elliptic curves. We analyse a possible way to extend their procedure to the complex case using results regarding the complex AGM due to Cremona and Thongjunthug in [CT13]. Even though the way of extending the procedure was the most intuitive one the algorithm does not work over the complex numbers, and we explain the reasons behind this. We then briefly specialize our computation to the real case, where the method works properly. We complete our description computing the non-archimedean components extending the algorithm introduced by Müller and Stoll in [MS16] to any number field. The two methods together give us an efficient algorithm to compute the canonical height of elliptic curves defined over a totally real field. The algorithm that is nowadays used to compute the canonical height is due to Silverman [Sil88], but when high precision of the output is required the computation of the archimedean terms is quite slow, whereas to compute the non-archimedean ones the factorisation of the discriminant is a necessary step that may slow down the entire process. Our aim is overcome these issues with new methods.

## 2.1 Archimedean terms

As we saw in Theorem 1.1.6, we can split the canonical height as a sum of local terms. We now focus at the archimedean places of the field $K$ of definition of the elliptic curve $E$. We fix one embedding $K \hookrightarrow \mathbb{C}$ and, applying it to the point and curve, we calculate the local archimedean height at that component.

In this way we reduce the problem to calculating the local height of a point $P$ on

a complex elliptic curve $E$. Afterwards, we just need to sum all the local archimedean components weighted by the local degree $n_v$.

The idea is to build a sequence of elliptic curves, connected by isogenies, which converge to a singular curve. Then, using the Theorem 1.2.7, we aim to deduce the value of $\lambda_v(P)$ by working backwards, starting from the limit value of the sequence of heights of points over the isogenous elliptic curves and tracking it back to $E$.

There is interest around these methods because the standard formulation of the local archimedean height involves the Weierstrass $\sigma$-function, as shown in [Sil99, §VI-3.2]. In one hand the formulation with the Weierstrass $\sigma$-function is more elegant from a theoretical point of view, on the other hand it is hard to compute and a new formulation, such the one described by Bost and Mestre in the real case, would let us calculate quickly and more efficiently the value of the local archimedean height in the archimedean case.

### 2.1.1 Reformulation of the local archimedean height

In this section we will study a chain of elliptic curves defined by an AGM-sequence as was done in [CT13]. Let us consider an elliptic curve $E_0$, defined over $\mathbb{C}$ by a Weierstrass model which contains the point $(0,0)$. Note that we can always reduce to this case by a translation, indeed, using the Corollary 1.2.8 the local height is preserved. Therefore, we can write the equation of $E_0$ as

$$E_0 : y^2 = x(x+e)(x+f),$$

where $e$ and $f$ are distinct, non zero complex numbers.

We want to compute the local archimedean height of a point $P_0 \in E_0$ by building a chain of elliptic curves and isogenies keeping track of the value $\lambda$. This sequence of elliptic curves will be defined by the *strongly optimal* (using the terminology of [CT13]) AGM-sequence applied to the square roots of $e$ and $f$.

**Definition 2.1.1.** *Given two complex numbers $(a_0, b_0)$ we define the AGM-sequence by*

$$a_n = \frac{a_{n-1} + b_{n-1}}{2} \qquad b_n^2 = a_{n-1}b_{n-1} \qquad n > 0,$$

*i.e. where $a_n$ and $b_n$ are the arithmetic and geometric mean of the previous terms. As defined in [CT13, §2] we say that if $b_n$ is such that*

$$\Re(b_n/a_n) \geq 0,$$

*we call this the* good *choice (between* $\pm b_n$*),* bad *otherwise. If at every step the choice is* good *the sequence is said to be* optimal*, and* strongly optimal *if in addition* $\Re(b_0/a_0) \geq 0$.

Therefore we define a strongly optimal AGM sequence starting from $a_0$ and $b_0$ such that

$$a_0^2 = e \qquad b_0^2 = f \qquad \Re(b_0/a_0) \geq 0.$$

By the terms $(a_i)_{i\in\mathbb{N}}$ and $(b_i)_{i\in\mathbb{N}}$ of the AGM sequence we define a family of elliptic curves $E_n$ described by the equations

$$y^2 = x(x + a_n^2)(x + b_n^2),$$

and family of 2-isogenies $\alpha_n : E_{n+1} \to E_n$ by

$$(x, y) \mapsto \left( x\frac{(x + b_{n+1}^2)}{(x + a_{n+1}^2)}, y\frac{(x + a_n a_{n+1})(x + b_n a_{n+1})}{(x + a_{n+1}^2)^2} \right).$$

To simplify the notation we refer to the local height function over $E_n$ as $\lambda_n$.

**Lemma 2.1.2.** *The isogenies* $\alpha_n$ *are normalized, i.e.* $c_\alpha = 1$.

*Proof.* Applying the notation used in Corollary 1.2.4 we have

$$c_{\alpha_n} = \frac{r_n'(x)}{s_n(x)} = \frac{x^2 + 2xa_{n+1}^2 + a_{n+1}^2 b_{n+1}^2}{(x + a_n a_{n+1})(x + b_n a_{n+1})} = 1.$$

□

Since $\deg(\alpha_n) = 2$ and $\ker(\alpha_n) = \{(-a_{n+1}^2, 0), O\}$, applying Theorem 1.2.7 we have

$$\lambda_n(\alpha_n(P)) = 2\lambda_{n+1}(P) + v(x(P) + a_{n+1}^2) \qquad \forall P \in E_{n+1}(\mathbb{C}) \setminus \ker(\alpha_n), \quad \forall n \geq 0. \tag{2.1}$$

Therefore, we have the following chain of elliptic curves and isogenies

$$E_0 \xleftarrow{\alpha_0} E_1 \xleftarrow{\alpha_1} E_2 \quad \cdots \quad \xleftarrow{\alpha_n} E_{n+1} \quad \cdots$$

Let us consider a sequence of points $(P_i)_{i\in\mathbb{N}}$, where $\alpha_n(P_n) = P_{n-1}$ for all positive $n$. Starting from a fixed point $P_0 \in E_0$ there are uncountably many such sequences. Indeed, for every $n$, there are two points on $E_{n+1}$ which are mapped in $P_n$ through $\alpha_n$ for all $n$. Setting $x_k = x(P_k)$, these two points have the following $x$-coordinates

$$x_{n+1} = \frac{1}{2}\left(x_n - a_n b_n + t_n\right),$$

where $t_n^2 = (x_n + a_n^2)(x_n + b_n^2)$. We have to choose which value of $t_n$ consider, again the *good* choice is taking the one such that $\Re(t_n/(x_n + a_n b_n)) \geq 0$. Recalling the definition of $v$ and defining $z_i = x_i + a_i^2$ to simplify the notation, the equation (2.1) becomes

$$\lambda_n(P_n) = 2\lambda_{n+1}(P_{n+1}) - \log|z_{n+1}|\,. \tag{2.2}$$

We want to make sure that the above is always defined, i.e. $z_{n+1} \neq 0$. This is not a lack of coherency in the equation (2.2): if $z_{n+1} = 0$ then $P_{n+1} \in \ker(\alpha_n)$ but $\lambda_n$ is not defined at the point $O$, so both sides of the equations are not defined. Actually all points of the sequence $(P_i)_{i\in\mathbb{N}}$ are not involved in this issue. Indeed, first notice that fixing a point $P_i$ in the sequence any previous element $P_j$ can be expressed as the image of $P_i$ through a composition of isogenies. Then, if $P_i$ has order at most 2 then $P_j$ has also order at most 2.

Since $z_n = 0$ implies that $P_n$ has order 2, if we start with a point not it $E_0[2]$, then $z_n \neq 0$ (and so $|z_n| \neq 0$) for all $n \geq 0$. So $|z_n|_{n\geq 0}$ is a sequence of positive real numbers.

The two sequences $(a_i)_{i\in\mathbb{N}}$ and $(b_i)_{i\in\mathbb{N}}$ converge quadratically to the arithmetic–geometric mean $M(a_0, b_0)$ (see [Dup06] for details) and therefore we can consider the limit of the elliptic curves sequence

$$E_\infty := y^2 = x(x + M(a_0, b_0)^2)^2.$$

The limit singular curve $E_\infty$ has a node in $(-M(a_0, b_0)^2, 0)$ and not a triple point since $M(a_0, b_0)$ is not 0, see [CT13] for details.

The sequence $(P_i)_{i\in\mathbb{N}}$ converges to a limit point $P_\infty$ on $E_\infty$. We want to consider the limit of the equation (2.2), but we need to check that $z_\infty := \lim_n |z_n|$ is not zero and that $\lim_n \lambda_n(P_n)$ converges to a value of $\lambda_\infty$. The fact that $z_\infty \neq 0$ comes from [CT13, Prop 25], using the change of coordinates $(x'_\infty, y'_\infty) = (x_\infty + \frac{2}{3}M(a_0, b_0)^2, 2y_\infty)$ to conform to their notation, in the proof of the proposition[1] we have $0 \neq x'_\infty + \frac{1}{3}M(a_0, b_0)^2 = x_\infty + M(a_0, b_0)^2 = z_\infty$. To prove the convergence of $\lim_n \lambda_n(P_n)$ we will use the following technical lemma based on the convergence rate of the AGM sequence. The choice of the series studied become clear later on.

[1] Here we can apply the proposition since $P$ is not a point order 2.

**Lemma 2.1.3.** *The series*

$$\sum_{i=1}^{\infty} 2^i \log\left|\frac{z_{i+1}}{z_i}\right|$$

*is convergent.*

*Proof.* Let us study the behaviour of $\left|\frac{z_{i+1}}{z_i}\right|$, all the following square roots are chosen referring to the definition above of *good choice*

$$\begin{aligned}
\left|\frac{z_{i+1}}{z_i}\right| &= \left|\frac{x_{i+1}+a_{i+1}^2}{z_i}\right| = \left|\frac{x_i + \frac{a_i^2+b_i^2}{2} + \sqrt{(x_i+a_i^2)(x_i+b_i^2)}}{2z_i}\right| \\
&= \left|\frac{x_i + a_i^2 - \frac{a_i^2-b_i^2}{2} + \sqrt{(x_i+a_i^2)(x_i+b_i^2)}}{2z_i}\right| \\
&= \left|\frac{2z_i - z_i - \frac{a_i^2-b_i^2}{2} + \sqrt{(x_i+a_i^2)(x_i+b_i^2)}}{2z_i}\right| \\
&\leq 1 + \left|\frac{b_i^2-a_i^2}{4z_i} + \frac{\sqrt{(x_i+a_i^2)(x_i+b_i^2)} - z_i}{2z_i}\right| \\
&= 1 + s_i,
\end{aligned}$$

where $s_i = \left|\frac{b_i^2-a_i^2}{4z_i} + \frac{\sqrt{(x_i+a_i^2)(x_i+b_i^2)}-z_i}{2z_i}\right|$. By triangle inequality we can also say $1 - s_i \leq \left|\frac{z_{i+1}}{z_i}\right|$, therefore we have

$$\log(1-s_i) \leq \log\left|\frac{z_{i+1}}{z_i}\right| \leq \log(1+s_i). \tag{2.3}$$

Now let us have a look at the terms of $s_i$

$$\frac{\sqrt{(x_i+a_i^2)(x_i+b_i^2)} - z_i}{2z_i} = \frac{\sqrt{z_i(x_i+b_i^2)} - z_i}{2z_i} \cdot \left(\frac{\sqrt{z_i(x_i+b_i^2)} + z_i}{\sqrt{z_i(x_i+b_i^2)} + z_i}\right) =$$

$$\frac{z_i(x_i+b_i^2) - z_i^2}{2z_i(\sqrt{z_i(x_i+b_i^2)} + z_i)} = \frac{(x_i+b_i^2) - z_i}{2(\sqrt{z_i(x_i+b_i^2)} + z_i)} = \frac{b_i^2-a_i^2}{2(\sqrt{z_i(x_i+b_i^2)} + z_i)}.$$

We can rewrite $s_i$ as follows

$$s_i = |b_i - a_i||b_i + a_i| \left| \frac{1}{2(\sqrt{z_i(x_i + b_i^2)} + z_i)} + \frac{1}{4z_i} \right|.$$

The last absolute value, when $i$ tends to infinity, behaves like $\frac{1}{2z_i}$. Above we have shown that $\lim_i |z_i| = z_\infty \neq 0$, so $\frac{1}{2|z_i|}$ is bounded. Therefore, since also $|b_i + a_i|$ is bounded and $|b_i - a_i| \to 0$, $s_i$ tends to 0. Therefore, applying the limit for $i \to \infty$ to the inequalities (2.3), we have

$$\lim_{i\to\infty} -s_i \leq \lim_{i\to\infty} \log \left| \frac{z_{i+1}}{z_i} \right| \leq \lim_{i\to\infty} s_i, \tag{2.4}$$

where actually the left and right limits are 0, therefore every term tends to 0. We define $t_i = 2^i s_i$, and it follows

$$\lim_{i\to\infty} t_i = \lim_{i\to\infty} 2^i s_i = \lim_{i\to\infty} 2^i |b_i - a_i||b_i + a_i| \left| \frac{1}{2(\sqrt{z_i(x_i + b_i^2)} + z_i)} + \frac{1}{4z_i} \right|.$$

The last two factors tend to a constant value $u$, therefore

$$\lim_{i\to\infty} t_i = u \lim_{i\to\infty} 2^i |b_i - a_i|. \tag{2.5}$$

Now we can study easily the behaviour of the terms $t_i$ using a bound related to the AGM series $(a_i, b_i)$ over the complexes from [Dup06]

$$|a_{i+1} - b_{i+1}| \leq \frac{1}{4m_i} |a_i - b_i|^2,$$

where $m_i = \min\{|a_i|, |b_i|\}$. Since the AGM sequence is good it has non-zero limit (see [CT13]), then $m_i$ converges to a non-zero value as well. Therefore, there exists a real number $\varepsilon > 0$ and an integer $N_\varepsilon$, such that $4m_i > \varepsilon$ for every $i > N_\varepsilon$.

If we consider a integer $\tau$ bigger than $N_\varepsilon$ such that $|a_i - b_i| < \varepsilon/2$ for all $i \geq \tau$, iterating the previous formula we have

$$|a_n - b_n| < \frac{1}{\varepsilon^{2^{n-\tau}-1}} (a_\tau - b_\tau)^{2^{n-\tau}} < \frac{\varepsilon}{2^{2^{n-\tau}}}.$$

This shows that the AGM converges doubly exponentially and so the limit in (2.5)

converges exponentially to 0. Clearly, the same applies for $-t_i$.

We can now describe the behaviour of the serie: by the inequalities from (2.4) we have that the terms of the series $2^i \log\left|\frac{z_{i+1}}{z_i}\right|$, since they are bounded between $-t_i$ and $t_i$, converge exponentially to 0 too. □

We can now compute $\lim_n \lambda_n(P_n)$ .

**Lemma 2.1.4.** $\lim_n \lambda_n(P_n) = \log(z_\infty)$,

*Proof.* Let us consider the sequence

$$\varphi_n = 2^n(\lambda_n(P_n) - \log|z_n|).$$

If we can show the convergence of this sequence then the result follow easily, indeed if $\lim_n 2^n(\lambda_n(P_n) - \log|z_n|) = l$ then $\lim_n \lambda_n(P_n) - \log|z_n| = 0$ and since $|z_i|_{i\in\mathbb{N}}$ converges to $z_\infty$ we would be done. Therefore, we will just need to prove the convergence of the sequence by showing that it is Cauchy. We can compute the difference between terms in the sequence by applying the formula (2.2):

$$\varphi_m - \varphi_n = \sum_{i=n}^{m-1} 2^i \log\left|\frac{z_i}{z_{i+1}}\right|.$$

The difference above satisfies the Cauchy condition since it is a negated partial sum of the tail of the sequence from Lemma 2.1.3. □

Finally, having computed the limit value, we can obtain the value of $\lambda(P_0)$ by iterating equation (2.2), which means

$$\begin{aligned}
\lambda_0(P_0) &= 2\lambda_1(P_1) - \log|z_1| \\
&= 4\lambda_2(P_2) - 2\log|z_2| - \log|z_1| \\
&= 8\lambda_3(P_3) - 4\log|z_3| - 2\log|z_2| - \log|z_1| \\
&\vdots \\
&= 2^n\lambda_n(P_n) - \sum_{i=1}^{n} 2^{i-1}\log|z_i|\,.
\end{aligned}$$

The expression above cannot be used directly to compute the local height. We now derive a reformulation that turns to be explicit in the real case but not in the complex one.

**Theorem 2.1.5.** *Let $E_0$ be a complex elliptic curve, with equation $E_0 : y^2 = x(x+e)(x+f)$. Then the local height of a point $P_0$ in $E_0 \setminus E_0[2]$ is*

$$\lambda_0(P_0) = \log|z_1| + \sum_{i=1}^{\infty} 2^i \log\left|\frac{z_{i+1}}{z_i}\right| + l, \tag{2.6}$$

*where $l = \lim_n 2^n\lambda_n(P_n) - 2^n\log|z_n|$ and $(z_i)_{i\in\mathbb{N}}$ is the sequence defined as $z_i = x_i + a_i^2$: the $x_i$ are the $x$-coordinates of the points in the sequence $(P_i)_{i\in\mathbb{N}}$ and $a_i^2$ are the coefficients from the models of the isogenous elliptic curves defined by the AGM-sequence.*

*Proof.* We know that $\lambda_0 = 2^n\lambda_n(P_n) - \sum_{i=1}^{n} 2^{i-1}\log|z_i|$, adding and subtracting $2^n\log|z_n|$ we can prove the convergence of this expression when $n$ tends to infinity, indeed we have

$$\begin{aligned}
\lambda_0(P_0) &= 2^n\lambda_n(P_n) - 2^n\log|z_n| + 2^n\log|z_n| - \sum_{i=1}^{n} 2^{i-1}\log|z_i| \\
&= 2^n\lambda_n(P_n) - 2^n\log|z_n| + \log\left|\frac{z_n^{2^{n-1}}}{\prod_{i=1}^{n} z_i^{2^{i-1}}}\right| \\
&= 2^n\lambda_n(P_n) - 2^n\log|z_n| + \log\left|z_1\prod_{i=1}^{n-1}\left(\frac{z_{i+1}}{z_i}\right)^{2^i}\right| \\
&= 2^n\lambda_n(P_n) - 2^n\log|z_n| + \log|z_1| + \sum_{i=1}^{n-1} 2^i\log\left|\frac{z_{i+1}}{z_i}\right|.
\end{aligned}$$

We already have $\lim_n 2^n\lambda_n(P_n) - 2^n\log|z_n| = l$ from the proof of Lemma 2.1.4 and the series $\sum_{i=1}^{\infty} 2^i\log\left|\frac{z_{i+1}}{z_i}\right|$ converges by Lemma 2.1.3, so if we let $n$ to $\infty$ the RHS converges to

$$\lambda_0(P_0) = \log|z_1| + \sum_{i=1}^{\infty} 2^i\log\left|\frac{z_{i+1}}{z_i}\right| + l.$$

□

*Remark* 2.1.6. The formula's rearrangement involving logarithm's properties is a key point for the explicit computation of it. Indeed, the limit

$$\lim_n \log\left|\frac{z_n^{2^n}}{\prod_{k=1}^{n} z_k^{2^{k-1}}}\right|$$

involves terms which grow very fast, which represent an issue when we actually want to compute it. On the contrary the formula (2.6) has smaller values, each term of the sum

is easier to compute and fewer values need to be stored in its computation.

Our initial goal was to show that $l = 0$ in the complex case but actually this is not true. The following observation about the value of the limit $l$ is due to Bill Allombert.

*Remark* 2.1.7. Consider the equation

$$\lambda_{n+1}(P_{n+1}) = \frac{\lambda_n(P_n) + \log|z_{n+1}|}{2}.$$

We know that $\log|z_n|$ converges quadratically to $\log|z_\infty|$, however it does not follow that $\lambda_n(P_n)$ converges quadratically to $\lambda_\infty(P_\infty)$. Indeed, as soon as $n$ is not too small, $\log|z_n|$ is nearly constant to $\log|z_\infty|$, so for large $n$

$$\lambda_{n+1}(P_{n+1}) \simeq \frac{\lambda_n(P_n) + \log|z_\infty|}{2},$$

which converges only linearly to $\log|z_\infty|$.

The convergence of the sequence

$$\varphi_n = 2^n(\lambda_n(P_n) - \log|z_n|)$$

is proven in the Lemma 2.1.4, but this only establishes the linear convergence of $\lambda_n(P_n)$.

To show that $\lambda_n(P_n)$ converges quadratically, one would need to show that $2^{2^n}(\lambda_n(P_n) - \log|z_n|)$ is bounded, but this fails to hold in the complex case. For instance, we have the following numerical example

*Example* 2.1.8. Consider the real elliptic curve $E$

$$E : y^2 = x(x-4)(x-9)$$

and the point $P = (1, 2\sqrt{6})$. Computing the values $\lambda_i(P_i)$ with the Silverman algorithm from [Sil88] and comparing them with the values $\log|z_i|$ we have

| $i$ | $\lambda_i(P_i)$ | $\log\|z_i\|$ |
|---|---|---|
| 1 | 1.96841926689722212837586022629430 | 1.98589072535329580623151374026941 |
| 2 | 1.96846380964664016567380307532308 | 1.96850835239605820297174592435186 |
| 3 | 1.96846380993658617708943370166023 | 1.96846381022653218850506432799739 |
| 4 | 1.96846380993658617710171937634008 | 1.96846380993658617711400505101993 |
| 5 | 1.96846380993658617710171937634008 | 1.96846380993658617710171937634008 |
| 6 | 1.96846380993658617710171937634008 | 1.96846380993658617710171937634008 |

Both sequences converge quadratically.

If instead we consider the same curve but running computations that involve complex numbers, such as the height of the point $Q = (-1, i5\sqrt{2})$ we have

| $i$ | $\lambda_i(P_i)$ | $\log\|z_i\|$ |
|---|---|---|
| 1 | 1.68899101331846299059200440392999 | 1.64856049438482233961656213215638 |
| 2 | 1.65653262948370061031919363133640 | 1.62407424564893823004638285874281 |
| 3 | 1.64027200837774462494733977911089 | 1.62401138727178863957548592688538 |
| 4 | 1.63214169762017826814656400947240 | 1.62401138686261191134578823983390 |
| 5 | 1.62807654224139508973750724842749 | 1.62401138686261191132845048738259 |
| 6 | 1.62604396455200350053297886790504 | 1.62401138686261191132845048738259 |
| 7 | 1.62502767570730770593071467764381 | 1.62401138686261191132845048738259 |
| 8 | 1.62451953128495980862958258251320 | 1.62401138686261191132845048738259 |
| 9 | 1.62426545907378585997901653494790 | 1.62401138686261191132845048738259 |
| 10 | 1.62413842296819888565373351116524 | 1.62401138686261191132845048738259 |
| 11 | 1.62407490491540539849109199927392 | 1.62401138686261191132845048738259 |
| 12 | 1.62404314588900865490977124332825 | 1.62401138686261191132845048738259 |
| 13 | 1.62402726637581028311911086535542 | 1.62401138686261191132845048738259 |
| 14 | 1.62401932661921109722378067636900 | 1.62401138686261191132845048738259 |
| 15 | 1.62401535674091150427611558187580 | 1.62401138686261191132845048738259 |

where $\lambda_i(P_i)$ converges only linearly.

It remains unclear why over the real numbers we have $l = 0$, indeed the convergence rate of the real AGM is the same one of the complex AGM.

Describing this algorithm over the reals neither Bost and Mestre in [BM], Müller and Stoll in [MS16] or Bradshaw in [Bra10] discussed the convergence of the formula (2.6). The limit $l$ was never taken in consideration in the previous works. Therefore this algorithm, that is currently used in PARI to compute the local height over the real places, has not been entirely proved to be true. On the other hand, computational evidence suggest that the limit $l$ should be zero over the real numbers.

### 2.1.2 Heuristics on the limit $l$

In order to study the limit value $l$ we have done some numerical experiments. Unfortunately the limit $l$ seems to be dependent on the curve and on the point. In particular, we can extrapolate from our experiments that:

- When the sequences of points and curves are real, the algorithm behaves properly, indeed it coincides with the Bost and Mestre one.
- We apply the algorithm to real points over real elliptic curves that are not in the identity component, i.e. the points that have the $x$-coordinate between $-a^2$ and $-b^2$. In Bost and Mestre's method, we are supposed to move the points to the other component, but here we are dealing with those points with the same "dignity": indeed we apply the same algorithm for every complex point (and so the real ones aforementioned). What happens is that the limit $l$ for those points seems to be constant (with respect to the points, not to the curve) but not zero.
- When the $x$-coordinate of the point $P$ is, in absolute value, considerably greater than $a$ and $b$ the limit $l$ gets smaller.
- By the equality (2.2) we have

$$l = \lim_n 2^n(\lambda_n(P_n) - \log|z_n|) = \lim_n 2^n(\lambda_{n-1}(P_{n-1}) - \lambda_n(P_n)).$$

  Therefore, the limit $l$ describes the variation of the archimedean height through the sequence of isogeneous elliptic curves. The sequence $(P_i)_{i\in\mathbb{N}}$ converges to a limit point $P_\infty$ on $E_\infty$, which is the limit curve of the sequence $(E_i)_{i\in\mathbb{N}}$. Both sequences converge double exponentially, since the terms of the sequences are described by terms of the AGM-sequence. In the real case the sequence $(\lambda_i(P_i))_{i\in\mathbb{N}}$ numerically converges double exponentially as well, and so $l = 0$. In the complex case the sequence $(\lambda_i(P_i))_{i\in\mathbb{N}}$ still converges but slowly, from which follows that $l \neq 0$. For instance, applying the algorithm in the complex case we construct sequences of

curves and points whose coefficients, after few steps, are equal up to hundreds of digits, whereas the difference between the archimedean heights is still consistent.

- Making bad choices in the AGM sequence leads to different limiting values. Indeed, in the real setting when bad choices are made the error scales exactly by a quadratic factor as a function of the number of bad choices and at which steps the bad choices are made. Even in the complex computations, for $x$-coordinates big enough with respect to $a$ and $b$, the limit behaves roughly quadratically with respect to the number and steps of the bad choices. The direct connection between the steps when a bad choice is made and the value of the limit is not clear, but roughly, the greater is $n$ such that the $n$-choice is bad the greater is the limit $l$.

## 2.2 Real case

Bost and Mestre described in [BM] an algorithm to compute the local height of a curve embedded in the real numbers. In the previous section we showed a possible generalisation to this algorithm that actually fails. Here we briefly recap how the precedure works over the reals, specialising the method introduced for the complex numbers.

### 2.2.1 Suitable configuration

In the complex case, the chain of isogenous elliptic curves $E_n$ was defined by the 2-torsion groups. In the real case we need curves with full 2-torsion group. Moreover, we will need the point $P$, for which we want to compute the local archimedean height, to lie in the identity component (the one that contains the point at infinity $O$). Additionally, we change coordinates in such a way that the biggest $x$-coordinate of the three real 2-torsion points be 0. So our aim is reducing the general case to the one above, while keeping track of the local height.

Let $(E, \omega)$ be an elliptic curve with its differential invariant and $P$ a point on it. Since the characteristic is 0, we can express $E$ with a short Weierstrass equation $E : y^2 = f(x)$, where $f(x)$ is polynomial in $x$ of degree 3, which has at least one real root, we pick $\bar{x}$ the maximum of them and change the model of $E$ mapping $x \mapsto x - \bar{x}$ and preserving the $y$-coordinate. We changed the model of the curve twice, but by Corrolary 1.2.8 the local and canonical heights are preserved. There are still two further steps to reach the aimed configuration.

In the case the elliptic curve $E$ has just one real point of 2-torsion its equation is

$$E : y^2 = x(x^2 + ux + v),$$

with $u^2 < 4v$. We can map $E$ to the 2-isogenous curve $E'$ given by

$$E' = E/\langle(0,0)\rangle = y^2 = x(x^2 - 2ux + u^2 - 4v)$$

that has 3 real 2-torsion points, via the isogeny $\alpha$ that maps

$$(x, y) \mapsto \left(\frac{x^2 + ux + v}{x}, y\frac{(x^2 - v)}{x^2}\right).$$

Since $c_\alpha = 1$ and $\ker(\alpha) = \{(0,0), O\}$ the formula from the Theorem 1.2.7 becomes

$$\lambda_{E'}(\alpha(P)) = 2\lambda_E(P) + \frac{1}{2}v(x(P)).$$

If on the new curve $E'$, the biggest $x$-coordinate of the 2-torsion real points is different from 0, we can change the coordinates as above preserving $\lambda$ (since the discriminant is preserved via translation).

In the case the point $P$ does not belong to the identity component we can consider $2P$ that is on the identity component. We keep track of the local height by the Theorem 1.2.7, it follows that

$$\lambda_{E'}(2P) = 4\lambda_E(P) + v(2y(P)).$$

### 2.2.2 The chain of real elliptic curves

The problem has been reduced to computing the local height of a point $P_0$ that belongs to the identity component of a real elliptic curve $E_0$ with full 2-torsion. Moreover, the biggest $x$-coordinate of the real 2-torsion is 0. Therefore, we have

$$E_0 : y^2 = x(x + a_0^2)(x + b_0^2),$$

where $0 < b_0 < a_0$ are real numbers. It follows that $E_0[2] = \{(0,0), (-a_0^2, 0).(-b_0^2, 0), O\}$.

We define the sequence of curves and the isogenies in a similar way to Section 2.1, where the main difference is the field of definition of the coefficients involved.

In particular, the real AGM-sequence is defined without choices:

**Definition 2.2.1.** *Let $a_0$ and $b_0$ two positive reals. The real AGM-sequence is defined*

*by*

$$a_n = \frac{a_{n-1} + b_{n-1}}{2} \qquad b_n = \sqrt{a_{n-1}b_{n-1}} \qquad \forall n > 0,$$

*where for $b_n$ we take the positive square root.*

We then define the sequence of isogenous elliptic curves $E_n$

$$E_n := x(x + a_n^2)(x + b_n^2),$$

linked by the isogenies $\alpha_n : E_{n+1} \to E_n$ which are defined, in the same way as in the complex case, as

$$(x, y) \mapsto \left( x\frac{(x + b_{n+1}^2)}{(x + a_{n+1}^2)}, y\frac{(x + a_n a_{n+1})(x + b_n a_{n+1})}{(x + a_{n+1}^2)^2} \right).$$

If we consider a point $P_n$ on the identity component of $E_n$ there is only one point $P_{n+1}$ in the identity component of $E_{n+1}$ such that

$$\alpha_n(P_{n+1}) = P_n,$$

therefore we can define a sequence $(P_i)_{i\in\mathbb{N}}$ uniquely determined by a point $P_0 \in E_0$ in the identity component. In this way, the terms $z_i = x(P_i) + a_i^2$ are always non-negative.

By the Theorem 2.1.5 it follows that in the real case

$$\lambda(P_0) = \log z_1 + \sum_{i=1}^{\infty} 2^i \log \frac{z_{i+1}}{z_i} + l,$$

where according to the statements in [BM], [MS16] and [Bra10] $l$ should be zero.

**Speed Test**

The canonical height is a key tool of several algorithms, for instance it is used in Zagier's method for finding integral points [Zag87]. In particular most of the algorithms need a high precision of the canonical height and therefore a high precision of the archimedean terms is required. Here we compare the algorithm by Silverman implemented in Sage and the Bost and Mestre's one. Timing is taken in milliseconds. The test was made with a few elliptic curves defined over the reals.

| Precision in bits | Silverman | Bost and Mestre |
|---|---|---|
| 100 | 1.46 | 0.10 |
| 200 | 3.03 | 0.14 |
| 400 | 8.43 | 0.24 |
| 800 | 30.5 | 0.46 |
| 1600 | 142 | 1.13 |
| 3200 | 812 | 3.48 |
| 6400 | 5500 | 10.7 |
| 12800 | 33700 | 35 |

We notice that the timing of Silverman's algorithm scales quadratically with the precision where as Bost and Mestre's one scales linearly. Moreover, already at "standard" values of the precision the Bost and Mestre's algorithm performs much better.

## 2.3 Non-archimedean terms

To compute the non-archimedean local heights we generalise the method introduced by Müller and Stoll in [MS16] to any number field. Combining the results obtained from the two methods we get an efficient and fast way to compute the canonical height over any totally real number field.

Recall we are looking at an elliptic curve $E$ over a number field $K$, given by a Weierstrass equation $W$ with coefficients in $\mathcal{O}_K$. A possible approach to compute the canonical height is working out the difference between it and the naive height, by the following formula proved in [CPS06]

$$h(P) - \hat{h}(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \Psi_v(P),$$

where $\Psi_v(P)$ are defined in 1.1. Splitting the sum into archimedean and non-archimedean places allows to describe a method to compute it efficiently. The non-archimedean contribution is

$$\Psi^f(P) := \sum_{v \in M_K^f} n_v \Psi_v(P) = \sum_{v \in M_K^f} \mu_v(P) \log(\#k_v),$$

where $M_K^f$ is the subset of the non-archimedean places in $M_K$ and $\mu_v$ is the local height correction function over $\mathbb{Q}_v$ defined in 1.2.

Although it is easy to compute $\mu_v(P)$ for each non-archimedean $v$, doing so requires having a model for $E$ which is minimal at $v$, so that the computation of $\Psi^f(P)$ in this way involves a possibly expensive factorization of the discriminant of the given model. We avoid this issue by computing directly the sum of the local terms generalising the algorithm from [MS16]. Fix the Kummer coordinates $(x_1 : x_2)$ of a point $P \in E(K)$. We assume that $(x_1 : x_2) \in \mathcal{O}_K$. The method described in [MS16] keeps doubling the point $P$ and computes the gcd of its coordinates; unfortunately this approach cannot be directly applied to any number field, since if $\mathcal{O}_K$ is not principal (i.e. the class number of $K$ is bigger than 1): we do not have in general a generator for the ideal $I_i = \langle x_i, y_i \rangle$, where $(x_i : y_i)$ are the Kummer coordinates of $2^i P$. A solution is, instead of dividing $x_i$ and $y_i$ by the greatest common divisor, "cleaning" the coordinates of primes of bad reduction, obtaining an ideal $J_i$ in the same class of $I_i$, which has valuation zero at the bad primes. Moreover, we will store the norm of the ideal, and not the ideal itself. Therefore, instead of dividing by the gcd, we consider an ideal which is coprime with the bad primes and belongs to the same class of the one generated by the two element. Let us now describe the procedure in more detail.

**Definition 2.3.1.** *Let $(x_1, x_2)$, with $x_1, x_2 \in \mathcal{O}_K$, be the Kummer coordinates of a point $P \in E(K)$ and $D$ an ideal in $\mathcal{O}_K$. There exists an $\alpha \in K^*$ such that $\alpha x_1, \alpha x_2 \in \mathcal{O}_K$ and the ideal $\langle \alpha x_1, \alpha x_2 \rangle$ is coprime to $D$. We refer to any such pair $(\alpha x_1, \alpha x_2)$ as* reduced *Kummer coordinates for $P$ with respect to $D$ and write*

$$r_D(x_1, x_2) := (\alpha x_1, \alpha x_2).$$

An algorithm to compute $\alpha$ may be found in [Coh00][1.3.14]. In case the ideal $\langle x_1, x_2 \rangle$ is principal with generator $g$ we simply take $\alpha = 1/g$.

Setting $D$ as $N(\Delta(W))$ computing $r_D(x_1, x_2)$ we obtain a new pair of Kummer coordinates for $P$ which have no bad primes in common: we have[2] $\min\{v(\alpha x_1), v(\alpha x_2)\} = 0$ for every $v$ dividing $N(\Delta(W))$. This procedure can be also described in terms of the ring $\mathcal{O}_{K,S}$ where $S$ is the set of primes which divides $N(\Delta(W))$.

The extended version of the code presented in [MS16] can be summarized as follows:

[2] actually we need just for the primes which divide $\Delta(W)$, but for the further computations it will be easier cleaning all the primes above $p|N(\Delta(W))$.

**Input** : A point $P$ on an elliptic curve $E$ over a number field $K$, given by a Weierstrass equation $W$ with coefficients in $\mathcal{O}_K$. The point $P$ is expressed with its Kummer coordinates $(x_1, x_2)$, with $x_1, x_2 \in \mathcal{O}_K$.

**Output**: The non-archimedean height $\Psi^f(P)$ of $P$.

$(x_1, x_2) \leftarrow r_{N(\Delta(W))}(x_1, x_2)$

$(x'_1, x'_2) \leftarrow \delta(x_1, x_2)$ We double the point P

$g_0 \leftarrow N(x'_1, x'_2)/N(x_1, x_2)^4$ We erase all the extra factors

$D \leftarrow N(\langle \Delta(W), g_0^\infty \rangle)$

$(x_1, x_2) \leftarrow r_D(x'_1, x'_2)$

$B \leftarrow \left\lfloor \dfrac{\log D}{\log 2} \right\rfloor$

**if** $B \leq 1$ **then return** 0

$m \leftarrow \left\lfloor \frac{\log([K:\mathbb{Q}]^3 B^5/3)}{\log 4} \right\rfloor$

**for** $n = 1$ *to* $m$ **do**

$(x'_1, x'_2) \leftarrow \delta(x_1, x_2)$

$g_n \leftarrow N(x'_1, x'_2)/N(x_1, x_2)^4$

$(x_1, x_2) \leftarrow r_D(x'_1, x'_2)$

**end**

Apply Bernstein's algorithm from [Ber05] to the $g_n$'s, obtaining a sequence of pairwise coprime integers $q_i$ such that $g_n = \prod_{i=0}^{r} q_i^{e_{i,n}}$ for every $n$.

**for** $i = 0$ *to* $r$ **do**

$a \leftarrow \sum_{n=0}^{m} 4^{-n-1} e_{i,n}$

$\mu_i \leftarrow$ simplest fraction between $a$ and $a + \frac{1}{B^4[K:\mathbb{Q}]^2}$

**end**

**return**

$\sum_{i=0}^{r} \mu_i \log(q_i)$

By simplest fraction we mean the fraction with the smallest denominator, which is unique. Indeed, in an interval of size $\frac{1}{B^4[K:\mathbb{Q}]^2}$, there is just one fraction whose denominator is bounded by $B^2[K:\mathbb{Q}]$. The code structure is essentially the same, the two differences being in the computation of the gcd and how we "clean" the coordinates, as compared to [MS16]. Indeed, here the Kummer coordinates $(x_1, x_2)$ are not necessarily coprime but, acting via the reduction $r_D$, just primes that are of good reduction and coprime with $g_0$ factor the ideal $\langle x_1, x_2\rangle$. So that, although at each stage there should be a correction term, we know for these primes that these correction terms add to 0 since the local height at such primes is 0, see [Sil99, 4.1.1]. By the argument above just primes of good reduction coprime with $g_0$ divide $N(x_1, x_2)$ and, since $\delta$ has degree 4, $N(x_1, x_2)^4$ divides $N(x_1', x_2')$; therefore, even though such primes do not contribute to the value of $\Psi^f(P)$, in the procedure we define $g_n$ as $N(x_1', x_2')/N(x_1, x_2)^4$, "cleaning" part of the primes of good reduction, in order to store and compute smaller terms.

Extending the computation to any number field is based on the equality

$$v_p(N(\mathfrak{p})) = v(p^{[k_\mathfrak{p}:\mathbb{F}_p]}) = \log_p(\#k_\mathfrak{p}),$$

where $k_\mathfrak{p}$ is the local ring $\mathcal{O}_K/\mathfrak{p}$. Indeed we will have for every ideal $I$ in $\mathcal{O}_k$

$$v_p(N(I)) = \sum_{\mathfrak{p}|p} v_\mathfrak{p}(I)\log_p(\#k_\mathfrak{p}),$$

which gives us for every $n \leq m$

$$v_p(g_n) = \sum_{\mathfrak{p}|p} \varepsilon_\mathfrak{p}(2^n P)\log_p(\#k_\mathfrak{p}), \tag{2.7}$$

which implies, recalling the notation used in [MS16],

$$\sum_{n=0}^{m} 4^{-n-1}\sum_{\mathfrak{p}|p}\varepsilon_\mathfrak{p}(2^n P)\log_p(\#k_\mathfrak{p}) = \sum_{n=0}^{m} 4^{-n-1}v_p(g_n) = b_p\sum_{n=0}^{m} 4^{-n-1}e_{i(p),n} = b_p a.$$

So we obtain

$$\sum_{\mathfrak{p}|p} \mu_{\mathfrak{p}}(P) \log_p(\#k_{\mathfrak{p}}) = \sum_{\mathfrak{p}|p} \sum_{n=0}^{\infty} 4^{-n-1} \varepsilon_{\mathfrak{p}}(2^n P) \log_p(\#k_{\mathfrak{p}})$$
$$= b_p a + \sum_{\mathfrak{p}|p} \sum_{n=m+1}^{\infty} 4^{-n-1} \varepsilon_{\mathfrak{p}}(2^n P) \log_p(\#k_{\mathfrak{p}}),$$

using (2.7), and $\varepsilon_p(g_n) \leq B$, we see that the last term in the sum lies in $\left[0, \frac{1}{B^4[K:\mathbb{Q}]^2}\right]$. So using the same argument from [MS16] we conclude that $\sum_{\mathfrak{p}|p} \mu_{\mathfrak{p}}(2^n P) \log_p(\#k_{\mathfrak{p}})/b_p$ is the unique fraction in $[a, a + \frac{1}{B^4[K:\mathbb{Q}]^2}]$ with denominator bounded by $B^2[K:\mathbb{Q}]$. Therefore we have

$$\Psi^f(P) = \sum_{v \in M_K^f} \mu_v(P) \log(\#k_v) = \sum_p \log(p) \sum_{\mathfrak{p}|p} \mu_{\mathfrak{p}}(P) \log_p(\#k_{\mathfrak{p}})$$
$$= \sum_p \log(p) \mu_{i(p)} b_p = \sum_{i=1}^{r} \mu_i \sum_{p|q_i} b_p \log(p)$$
$$= \sum_{i=1}^{r} \mu_i \log(q_i).$$

By this method we can compute all the contributions of the non-archimedean terms at once instead of factoring the discriminant of the elliptic curve $E$ as in Silverman's algorithm [Sil88]. Then, adding the archimedean local heights computed with the algorithm described in the previous section, we obtain the canonical height.

In particular, Müller and Stoll analysed in Chapter 7 of [MS16] how the algorithm performs in the case of a rational elliptic curve, with much shorter timings than Silverman's method. For elliptic curves defined over totally real fields we do expect similar performances.

# Part II

# The local solubility of plane quartics

# Chapter 3

# The density of everywhere locally solvable plane quartics

## 3.1 Introduction

A key information when we start to look for a solution to a specific equation, apart from the equation itself, is *where* we want to find a solution. Indeed, in most of the cases, the ring where we set our search changes the size of the set of the solutions. For example, if we have a polynomial in $\mathbb{Q}[x]$ that has a rational zero $\overline{x}$, we can obviously read $\overline{x}$ as a real or a $p$-adic number by the embeddings of $\mathbb{Q}$ in its completions. So, starting from a *global* solution, i.e. a solution defined over $\mathbb{Q}$ of a rational equation, we have *local* solutions at every completion, what about the converse? Given a rational equation, which we embeed in all the completion of $\mathbb{Q}$, can we start from all the local solutions (assuming they exist!) and build a global one? When this property is satisfied by a family of equations we say that the Hasse principle applies for the family. Unfortunately (or fortunately?) this principle does not apply for every type of equation, indeed we can show counterexamples even for univariate polynomials, such as

*Example* 3.1.1. Let $f(x) \in \mathbb{Z}[x]$ be the polynomial

$$f(x) = (x^2 - 2)(x^2 - 17)(x^2 - 34).$$

$f$ has no rational zeros but it has solutions over $\mathbb{R}$, and over $\mathbb{Q}_p$ for any $p$. Indeed for $p$ odd, a square root of an integer $n$ is an element of $\mathbb{Q}_p$ if $n$ is a quadratic residue mod $p$. So, if any of 2,17 and 34 has a square root in $\mathbb{Q}_p$ we have solubility in the $p$-adic field. The Legendre symbol $\left(\frac{a}{p}\right)$ is a function over the integers which is equal to 0 if $p|a$,

otherwise is $+1$ if $x^2 = a \mod (p)$ has a solution and $-1$ if it has no solutions. By the fact that this function is totally multiplicative we have

$$\left(\frac{2}{p}\right)\left(\frac{17}{p}\right) = \left(\frac{34}{p}\right).$$

For $p \neq 2, 17$ we always have one of the terms in the equation equal to 1, so $f$ has a solution in $\mathbb{Q}_p$ for $p \neq 2, 17$. For $p = 17$ we notice that $6^2 = 2 \mod 17$. For $p = 2$ the square root of $n$ exists if $n = 1 \mod 8$, therefore $\sqrt{17} \in \mathbb{Q}_2$.

It follows that $f$ has a zero in every completion of the rational numbers. Even though the equation $f$ has local solutions everywhere, it has not a global one.

One of the most famous theorem regarding the Hasse principle is the following:

**Theorem 3.1.2** (Hasse–Minkowski)**.** *A quadratic form with rational coefficients has a non-trivial zero over $\mathbb{Q}$ if and only if it has a zero over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all primes $p$.*

Unfortunately this result cannot be extended to the cubic case, indeed from the work of Selmer [Sel51], we have

**Theorem 3.1.3** (Selmer)**.** *The equation $3x^3+4y^3+5z^3 = 0$ has only the solution $(0, 0, 0)$ over $\mathbb{Q}$, but it has a non-zero solution over $\mathbb{R}$ and $\mathbb{Q}_p$ for every $p$.*

Moreover, in a recent work [BCF15a] Bhargava, Cremona and Fisher computed the probability that a cubic plane curve defined over $\mathbb{Q}$ is everywhere locally solvable, providing an exact formula. From this result the first author was able to deduce the following theorem:

**Theorem 3.1.4** (Bhargava)**.** *A positive proportion of plane cubics fail the Hasse principle.*

The principal aim of Part II of this thesis is to extend the work in [BCF15a] to the case of plane quartics, computing the density of these curves which have a point in each completion of $\mathbb{Q}$. We remark that we are not investigating the solubility over the rationals, but only local solubility.

## 3.2 Settings and procedure

The main object of our study will be homogeneous ternary quartic forms $T$, which locus is defined by a polynomial $f \in \mathbb{Q}[X, Y, Z]$. These quartics have 15 coefficients, which we can rescale in such a way they are integers and with great common divisor equal to

1. Our goal is to understand how many of them have solutions over $\mathbb{R}$ and $\mathbb{Q}_p$ for any $p$, we define this property as

**Definition 3.2.1.** *A polynomial that has zeros in all the completions of* $\mathbb{Q}$ *is* everywhere locally soluble.

It is necessary to formalise the concept "how many" since this set of curves is not finite. Ordering the plane quartics by the maximum of the absolute values of the coefficients makes it possible to describe a density over this family. Poonen and Voloch in [PV04] defined the probability $\rho$ that a random quartic is everywhere locally soluble.

**Definition 3.2.2.** *We define the density* $\rho$ *of everywhere locally soluble integral plane quartics* $T$ *as*

$$\rho := \lim_{B\to\infty} \frac{\#\{T : \text{ is everywhere locally soluble and } h(T) < B\}}{\#\{T : h(T) < B\}},$$

*where* $h(T) := \max\{|c|, \forall \text{ coefficient } c \text{ of } T\}$.

Notice that, for fixed $B$, the two sets in the definitions are finite, since we are considering plane quartics $T$ whose coefficients are integral.

In the same work [PV04] the two authors provided an important Theorem regarding the dependency of the solubility between all the completions of the rationals: actually they are independent. Without introducing their setting, their Theorem 3.6 can be read in our case (using $n = 2$ and $d = 4$ with respect to their notation) as:

**Theorem 3.2.3** (Poonen and Voloch)**.** *Let* $\rho(p)$ *be the probability (with respect to the usual Haar additive* $\mathbb{Z}_p$ *measure) that a random plane quartic form over* $\mathbb{Z}_p$ *is soluble over* $\mathbb{Q}_p$ *and let* $\rho(\infty)$ *be the probability over* $\mathbb{R}$ *with respect to the uniform distribution on the hypercube* $[-1, 1]^{15}$*, then*

$$\rho = \rho(\infty) \prod_p \rho(p).$$

By the above formula we can treat the computations independently, working out the solubility at each place of the rationals and then consider the product.

In order to describe the probability that a rational plane quartic is everywhere solvable we separate the computation into real and $p$-adic places. This division comes from the fact that the topology and, therefore, the methods are totally different between $\mathbb{R}$ and $\mathbb{Q}_p$.

The probability that a quartic is everywhere soluble depends on the distributions we consider for the space of the coefficients of the quartic, our aim is to pick the most "natural" one, even though one can argue that being "natural" is not at all a well-defined concept. We fix, as distribution $E$ on the space of the coefficients of the real ternary quartics, a piecewise smooth rapidly decaying function whose integral on $\mathbb{R}^{15}$ is 1. Then we can define the probability of solubility over the extension field $K$ of $\mathbb{Q}$ with respect to $E$ as:

**Definition 3.2.4.** *The probability $\rho^E(K)$ that a random integral quartic, with respect to the distribution $E$, is soluble over $K$ is*

$$\rho^E(K) := \lim_{X\to\infty} \frac{\sum_{T\in\mathbb{Z}^{15} \text{ and soluble over } K} E(T/X)}{\sum_{T\in\mathbb{Z}^{15}} E(T/X)}.$$

From [BCF+15b] we have a generalised version of Theorem 3.2.3. There the authors stated the theorem just in the case of $n$-ary quadrics but their arguments can be generalised to any degree.

**Theorem 3.2.5** (Bhargava, Cremona, Fisher)**.**

$$\rho^E = \rho^E(\mathbb{R}) \prod \rho^E(\mathbb{Q}_p) = \rho^E(\infty) \prod \rho(\mathbb{Q}_p),$$

*where $\rho^E(\infty) = \int_L E(T)dT$ with $L = \{T \in \mathbb{R}^{15}$ soluble on $\mathbb{R}\}$.*

This result is important for two reasons. First, the probability of solubility over the $p$-adic fields is independent of the choice of the distribution $E$. Indeed, it is proved in [BCF+15b] that the probability is equal to the one computed with respect to the usual additive measure on $\mathbb{Z}_p^{15}$. Then, it allows us to reformulate the probability of solubility of an integral ternary quartic $\rho^E(\mathbb{R})$ over the real numbers in terms of another family of ternary quartics.

In the case of the non-archimedean places, fixing a prime $p$, we want to compute the probability that a random homogeneous rational plane quartic $T$ has a zero over $\mathbb{Q}_p$. In order to do so we embed the rational quartic in $\mathbb{P}^2(\mathbb{Q}_p)$ and, after suitable rescaling, we assume that $f \in \mathbb{Z}_p[X,Y,Z] \setminus p\mathbb{Z}_p[X,Y,Z]$, i.e. the valuations of all the coefficients are non-negative and at least one of them is zero.

Considering the reduction $\overline{T}$ mod $p$ of the quartic $T$, we can extrapolate information on the solubility of $T$ itself. If $T(\mathbb{Q}_p) \neq \emptyset$ then its reduction $\overline{T}$ will have a point in $\mathbb{P}^2(\mathbb{F}_p)$. This does not characterise the solutions on $\mathbb{Q}_p$ but, by Hensel's Lemma, we have that if $\overline{T}$ has a smooth point over $\mathbb{F}_p$ then we can lift it to a $\mathbb{Q}_p$-point. Therefore, our

aim is to classify and count all the possible reduction types of $T$. In particular we are interested in distinguishing the following three cases:

- $\overline{T}(\mathbb{F}_p)$ is empty, hence so is $T(\mathbb{Q}_p)$;
- $\overline{T}(\mathbb{F}_p)$ contains a smooth point, then it lifts and $T(\mathbb{Q}_p) \neq \emptyset$;
- $\overline{T}(\mathbb{F}_p)$ consists of singular points only.

The quartics in the first set have probability of solubility 0, whereas the quartics from the second one have probability of solubility 1. In the last case we will *blow up* the singularities in a recursive fashion in order to understand whether the lift has a point defined over $\mathbb{Z}_p$. This procedure lets us compute the probability of solubility with respect to the reduction type of the quartic. We refer to the cases for which solubility is 1 as *good cases*, the cases with solubility 0 are called *bad* and the ones which need further investigation are called *undetermined*. Therefore, once we have divided all the reductions into the 3 sets above and understood *how many* curves there are in each set, we compute the solubility of the undetermined ones.

Even though in the cubic case it has been proved in [BCF15a] that there exists a single rational function in $p$, for $p$ big enough, that describes the density $\rho(p)$, it is not known in general whether such a rational function exists, especially in the case of quartics. According to Denef and Loeser in [DL01], $\rho(p)$ can be represented by a rational function of the counts of $\mathbb{F}_p$-points on a finite number of $\mathbb{Z}$-schemes.

In this work, in some cases the probability of solubility will be given as a rational function of $p$, which is valid for all $p \geq p_0$, where $p_0$ depends on the case. In other cases we will estimate the probability of solubility by only lower and upper bounds, each also being given by rational functions of $p$ and only valid for $p \geq p_0$.

*Conventions:* The curves we deal with are curves defined over $\mathbb{Q}$ by single homogeneous equation in $X$,$Y$ and $Z$. We will always assume that the equations are scaled to have integral and coprime coefficients. Hence, there is a well-defined reduction map

$$C(\mathbb{Q}_p) \to \overline{C}(\mathbb{F}_p)$$

whose image contains all smooth points. The complicated part is deciding whether a singular point in $\overline{C}(\mathbb{F}_p)$ is in the image of the reduction, we refer to this decision process as determining the "liftability" of a point in $\overline{C}(\mathbb{F}_p)$. Moreover, sometimes we will refer to the probability of solubility of a specific reduction just as solubility.

We briefly describe the structure of the following chapters. Chapter 4 is about methods to estimate the probability of solubility over the reals. Chapter 5 is dedicated to the classification and counting of all possible reductions mod $p$ of quartics over $\mathbb{Q}_p$. In Chapter 6 we focus on the non-reduced cases, i.e. when the reduction is a non-reduced curve, analysing the dependencies between the probabilities of liftability of the singular points. Chapter 7 is dedicated to the computation of the solubility probabilities in all cases where the reduction is semi-stable. Chapter 8 deals with non-semistable reductions. In Chapter 9 we conclude collecting all the local formulas to compute the density of everywhere locally soluble quartics.

# Chapter 4

# Real density

In this chapter we focus on the real case, embedding the rational quartics in the real projective plane $\mathbb{P}^2(\mathbb{R})$. We rescale the quartic in such a way that it is integral and that the coefficients have the greatest common divisor equal to 1.

By the arguments shown in the section 2 of [BCF$^+$15b] we know that, fixing the distribution $E$, the probability that a random integral form is soluble over $\mathbb{R}$ is equal to the probability that a random real form is indefinite. The argument described in the paper is specific for quadratic forms but it can be generalised to any degree. Notice that the two sets, whose probability we are evaluating, are not contained one in the other: the semi-definite positive or negative integral quartic forms are certainly soluble, but they are obviously not contained in the set of indefinite real ones. This argument works because the semi-definite ones are singular and therefore their density is zero with respect to $E$.

Indeed, we can show that semi-definite implies singular by the following argument. Suppose $T$ is a semi-definite quartic, which is zero at the point $P \in \mathbb{P}^2(\mathbb{R})$, by a change of coordinates we move $P$ to $[0:0:1]$, therefore $T$ is defined by the quartic:

$$Z^3C_1(X,Y) + Z^2C_2(X,Y) + ZC_3(X,Y) + C_4(X,Y) = 0,$$

where $C_i$ are binary forms of degree $i$. In this way, fixing $X$ and $Y$, we obtain a polynomial of odd degree in $Z$, which is indefinite. It follows that, since $T$ is semi-definite, $C_1$ has to be identically zero and so $T$ is singular in $[0:0:1]$. Therefore, not all soluble forms are indefinite, but the contribution, in terms of density, of the semi-definite ones is zero. By these considerations we can compute the solubility over the reals looking at the real quartics instead of the rational ones.

Computing the probability $\rho_i^E$ that a random real quartic is indefinite, with re-

spect to the distribution $E$, is equivalent to computing the probability it is positive definite $\rho_+^E$. Indeed, by symmetry the latter is equal to the probability of being negative definite, and therefore we have the relation between the two probabilities:

$$\rho^E(\mathbb{R}) = \rho_i^E = 1 - 2\rho_+^E.$$

Now we can restrict our study to $\rho_+^E$. We will evaluate lower and upper bounds for it which will lead to respectively upper and lower bounds for $\rho_i^E$.

## 4.1 The definite positive ternary quartics

Let us consider the 15-dimensional space of the coefficients for ternary quartics together with $l$, the function that sends a 15-dimensional vector to the associated quartic, with respect to the lexicographical order:

$$l : [a_1, \ldots, a_{15}] \longmapsto a_1X^4 + \ldots + a_{15}Z^4.$$

Our aim is to study the locus $D$, inside $\mathbb{R}^{15}$, of the definite positive real quartics. This locus $D$ describes a convex half-cone; indeed, if $f, g \in D$ then $tf + (1-t)g \in D$ for any $t \in [0,1]$ by the fact that the sum of definite forms is also a definite form. By the Bolzano–Weierstrass theorem any quartic attains a minimum (and a maximum) over the unit 3-dimensional sphere. We then define a function $m$ which sends a ternary quartic to its minimum value on the sphere. The function $m \circ l : \mathbb{R}^{15} \to \mathbb{R}$ is continuous. Moreover, the function $m \circ l$ is positive in $D$, negative over $\mathbb{R}^{15} \setminus \overline{D}$ and, by continuity, the boundary of $D$ is the locus of zero of this function, i.e. the set $\delta D$ of semi-definite positive quartics.

Since the boundary $\delta D$ is a hypersurface it has volume 0, so it has no contribution in the computation of the density of positive definite quartics. It follows that we can work with the convex and closed half-cone $\overline{D}$ of definite and semi-definite positive quartics.

An interesting and useful characterization of the points of the half-cone $\overline{D}$ is due to Hilbert in [Hil88]:

**Theorem 4.1.1** (Hilbert)**.** *Every non-negative real quartic form is the sum of three squares of quadratic forms.*

Actually, Hilbert's theorem is more general; it describes all the cases where the non-negative forms are characterised as sum of squares:

**Theorem 4.1.2** (Hilbert)**.** *The non-negative forms are the same as the sums of squares if and only if we are in one of the following three cases:*

- *binary forms (any degree);*
- *quadratic forms (any number of variables);*
- *ternary quartics.*

It is notable that the ternary quartics represent an "isolated" case.

Hilbert did not provide explicit counter-examples for all the other cases. For instance, if we consider

$$f(x,y,z) = z^6 + x^4y^2 + x^2y^4 - 3x^2y^2z^2,$$

it is a non-negative form but it cannot be written as sum of squares of cubic forms. This example is given by Motzkin in [Mot67]. One can show that $f$ is non-negative by noticing that it can be written as

$$f(x,y,z) = 3\left(\mathrm{AM}(z^6, x^4y^2, x^2y^4) - \mathrm{GM}(z^6, x^4y^2, x^2y^4)\right),$$

where AM stands for Arithmetic Mean and GM for Geometric Mean, then by the inequality involving the two means we conclude. To show that it cannot be written as sum of squares it is enough to show that a negative coefficient of $x^2y^2z^2$ cannot be achieved.

Since there is no direct method to test the positivity of a quartic (see [Nie12] ), such as the discriminant for univariate quadrics, using Hilbert's Theorem represents one of the few ways to tackle our problem. We can rewrite our half-cone as:

$$\overline{D} = \left\{a^2 + b^2 + c^2, \text{ where } a, b \text{ and } c \text{ are ternary quadrics}\right\}.$$

Unfortunately it is still hard to determine if a given form can be written as a sum of squares; there are methods that face this problem using semi-definite programming, details can be found here [**?** ]. Most of these methods treat the single curve, giving a rather slow algorithm to understand if it is a sum of squares or not. It turns out that these methods cannot be used directly to characterise the elements of $\overline{D}$ and evaluate its density in $\mathbb{R}^{15}$.

## 4.2 Computation of $\rho_+$

In order to compute the density of positive definite quartics we need to fix the distribution $E$. We choose to fix $E$ as the uniform distribution on the 15-dimensional unit hypercube. This is the same choice made by Poonen and Voloch in [PV04]. From

now on we do not emphasize in the notation the dependency of the probability on the distribution $E$, since it will not change.

To compute the probability $\rho_+$ we estimate the volume of the intersection of the convex half-cone $\overline{D}$ with the 15-dimensional hypercube $H$ inside $\mathbb{R}^{15}$. As stated in [Nie12] there are no closed equations that characterise the points inside the cone $\overline{D}$; otherwise we could have computed the probability $\rho_+$ by integration techniques. In the following sections we describe upper and lower bounds for the volume of $\overline{D}$. Moreover, we estimate the volume using a Monte Carlo's simulation.

### 4.2.1 Known results

This problem is rather specific but there is some previous work on it. The most interesting work in this direction uses the Löwner and John ellipsoids, which we now discuss briefly.

**Definition 4.2.1.** *Let $C$ a convex body in $n$-dimensional space. The John ellipsoid is the ellipsoid of maximal volume contained in $C$. The Löwner ellipsoid is the one of minimal volume that contains $C$.*

These two ellipsoids are unique, see [Bal97]. Grigoriy Blekherman in his work [Ble04] computed the Löwner and John Ellipsoids of the intersection between the Sum-of-squares cone and the hyperplane of all quartic forms with unit integral on the unit sphere, with respect to the metric induced by the natural inner product of the $n$-forms. The two ellipsoids are balls both centred on the point corresponding to the quartic $(x^2+y^2+z^2)^2$; they have respectively radius $\sqrt{14}$ and $1/\sqrt{14}$ with respect to the metric described in the paper.

Considering the cone with vertex in the origin and base the John Ellipsoids we obtain a cone that contains $D$. In a similar way, constructing a cone with base the Löwner ellipsoid, we get a cone that is contained in $D$. Computing the volume of these cones with respect to the uniform distribution $E$ we obtain an upper bound and a lower bound for the volume of $D$ itself, but unfortunately the bounds are not at all sharp.

### 4.2.2 Lower bound for $\rho_+$

We restrict our computation to the 15-dimensional hypercube, since $D$ is a half-cone, we can rescale each element to be inside the hypercube $H$ to be described by

$$H = \Big\{ -1 \leq x_i \leq 1, \forall i \in \{1, \dots, 15\} \Big\} \subset \mathbb{R}^{15}.$$

Considering the intersection $I = H \cap \overline{D}$, since $\overline{D}$ and $H$ are convex sets, $I$ is also convex. We want to determine a lower bound for the volume of $I$ by considering a convex hull of a set $S$ of points of $I$, being the aim to pick these points in such a way as to maximize the volume of the convex hull $\mathrm{Conv}(S)$. Since $\mathrm{Conv}(S)$ is obviously contained in $I$, adding elements to $S$ in order to achieve a bigger volume for $\mathrm{Conv}(S)$ means obtaining a sharper lower bound for $I$. The cone's vertex, the null vector representing the null quartic, is contained in $I$, therefore is natural to add it to the set $S$. Since $\overline{D}$ is a half-cone we only need to pick points on the surface of $H$ intersecting $\overline{D}$. There are two strategic types of points we consider:

- the vertices of $H$ inside $\overline{D}$;
- the points in the intersection between the two boundaries $\delta H$ and $\delta D$.

If we consider the convex hull of these points and the origin we will obtain $\overline{D}$ itself. The set $S$, defined in this way, is an infinite set and therefore working out of the volume of $\mathrm{Conv}(S)$ is not achievable from a computational point of view. We then pick a finite subset of the one described above.

The vertices of the hypercube $H$ are finite, so are the ones inside $\overline{D}$. Since there are just $2^{15}$, it is computationally feasible to test if each individual vertex is a sum of square or not using the Matlab free toolbox SOSTOOLS [PAV$^+$]. We obtained a list of 772 vertices of $H$ inside $\overline{D}$, and so initialised $S$ by adding these vertices. Then, adding to $S$ the origin, the convex hull of $S$ has still volume zero, since it has dimension 12 in a 15-dimensional space. Therefore, we still need to add to $S$ points that are in the intersection of the two boundaries. We now describe a method to pick elements in this intersection.

Let us consider a point $P$ on the boundary of $D$. If we consider its associated quartic $f$, it is semi-definite, so there exists a point in real space $(x, y, z) \in \mathbb{R}^3$ such that $f(x, y, z) = 0$. Moreover, by Hilbert's Theorem 4.1.1, $f$ can be expressed as a sum of 3 squared quadrics $a$,$b$ and $c$, i.e. $f = a^2 + b^2 + c^2$. This leads us to the conclusion that

$$a(x, y, z) = 0 = b(x, y, z) = c(x, y, z).$$

Therefore, we can characterise a quartic on the boundary as sum of 3 quadrics squared, which have a common zero. At this stage we can easily generate many points on the intersection: we pick a random point in $\mathbb{R}^3$ and we generate 3 random quadrics, passing through that point, summing their squares and converting the result into a vector with respect to the lexicographical order gives us a point that we add to $S$. Each time we

perform this procedure we enlarge $S$; its volume is bounded by the volume of $I$, therefore at each step we obtain a sharper lower bound for the volume of $I$.

An issue comes from the fact that the estimate of the volume is extremely expensive from a computational point of view. Indeed, the starting convex hull is already defined by hundreds of points in a 15-dimensional space. Moreover, in order to have a sensible result in terms of lower bound we need to add a large number points to $S$, probably in the order of hundreds of thousands. Unfortunately this is not computationally feasible, indeed the computation of the volume of the convex hull scales rapidly with the number of points that generates it. Using only the software VINCI [BA] we were able to compute just a really small lower bound, $\rho_+ > 1.513 \cdot 10^{-8}$, estimating the volume of a convex hull of a set $S$ containing roughly one thousand points.

### 4.2.3 Upper bound for $\rho_+$

Working out an upper bound for the volume of the cone $\overline{D}$ will lead us to a lower bound for the probability $\rho$ that a random quartic is indefinite. A possible approach to estimate the volume of the sum-of-squares cone is sequentially to cut the 15-dimensional hypercube $H$ by hyperplanes, and consider the intersection of the half-spaces where the cone is contained. A hyperplane can be defined evaluating a generic quartic (defined by 15 variables corresponding to the 15 coefficients) at a point of $\mathbb{R}^3$. The half-space where this linear polynomial in 15 variables is non-negative contains the cone. Varying the point where we evaluate the generic quartic we obtain different hyperplanes. Intersecting the half-spaces we obtain a convex region that contains the cone. Intersecting it with hypercube $H$, we can compute an upper bound for the proportion of quartics that are positive definite.

In order to compute an explicit upper bound we used the software VINCI [BA]. Taking as input the linear equation defining the hyperplanes and the hypercube the software is able to compute the volume of intersection region. Unfortunately, the complexity scales even more rapidly than in the previous case: we were able to obtain an answer after months of computation intersecting just 40 half-spaces. The upper bound obtained for the probability that a random real quartic is positive or semi-positive definite is

$$\rho_+ \leq 0.02493183808.$$

### 4.2.4 Estimating $\rho_+$ numerically

Unfortunately, the previous methods seemed quite hard from a computational point of view. In order to estimate the volume we performed a Monte Carlo simulation. We pick random quartics inside the hypercube $H$ and count the proportion of them that are positive or semi-positive definite. To detect if a given quartic is inside the cone $\overline{D}$ we can proceed in two ways:

- check if the associated polynomial can be expressed as a sum of squares;
- apply Seidenberg's algorithm; that detects if a real plane curve has points or not.

The second method is described in [Sei54]. It involves just the computation of the greatest common divisors, resultants and the Sturm function (which counts the number of real zero of a univariate polynomial). Instead, checking if a polynomial can be expressed as a sum of squares, cannot be performed in polynomial time, see [BS14] and [PW98]. It follows that Seidenberg's algorithm is, between the two methods mentioned above, the faster routine that let us distinguish between points inside and outside the cone. Hence, running a Monte Carlo that runs through over 100 millions of plane quartics, we estimated the proportion of positive and semi-positive quartics to be $\rho_+ \simeq 0.01038$.

## 4.3 Results on $\rho(\mathbb{R})$

From the computations of the previous sections we can deduce some results about $\rho(\mathbb{R})$. By the formula $\rho(\mathbb{R}) = 1-2\rho_+$, that links the probability of solubility of an integral ternary quartic to the probability that a real quartic is indefinite, we have then that

$$0.975068161914319 \leq \rho(\mathbb{R}) \leq 0.9999999684.$$

Moreover, by the Monte Carlo's simulation, we expect the actual value to be approximately

$$\rho(\mathbb{R}) \simeq 0.9792.$$

# Chapter 5

# Counting plane quartic curves

In this chapter we classify and count the different types of reductions of a plane quartic curve over $\mathbb{Q}_q$, for $q = p^l$ a prime power, where by $\mathbb{Q}_q$ we mean the unique unramified extension of degree $l$ of $\mathbb{Q}_p$. This is the first step towards the computation of the probability of solubility over $\mathbb{Q}_q$. Once we will have divided the reductions by their geometric invariants and counted them, in the next chapters we will compute the probability of solubility of each single case; then, gathering together all the information, we obtain an expression for the overall probability of solubility.

In this chapter we will study all the possible types of reduction of a plane quartic curve defined over the ring of integers $\mathbb{Z}_q$ of $\mathbb{Q}_q$, i.e. all the possible plane quartics defined over the residue field $\mathbb{F}_q$. Our aim is to classify these reductions and count them, expressing the results by polynomials in $q$. Here $q$ is a power of a rational prime number, when we will compute the probability of solubility we will restrict our arguments to just prime fields.

Some of the methods shown here, especially the techniques used to count the reducible reductions, are inspired by the computations in [BCF15a] for cubic curves. We begin with counting reducible curves.

## 5.1 Reducible Quartics count

In order to compute the number of quartic curves in $\mathbb{P}^2(\mathbb{F}_q)$ according to their geometric structure we recall and generalise two notation introduced in [BCF15a]:

**Proposition 5.1.1.** *The number of degree $k$ curves defined over $\mathbb{P}^2(\mathbb{F}_{q^j})$ is*

$$n_k^{(j)} = \frac{q^{j(k+1)(k+2)/2} - 1}{q^j - 1}.$$

*In the case $j = 1$ we will often write $n_k^{(j)}$ just as $n_k$ to simplify the notation.*

**Definition 5.1.2.** *We denote the number of points on $\mathbb{P}^m(\mathbb{F}_{q^j})$ as*

$$t_j^{(m)} = \sum_{i=0}^{m} q^{ij}.$$

*In the case $m = 2$ we will often write $t_j^{(m)}$ just as $t_j$ to simplify the notation.*

We want to count how many quartics are defined over $\mathbb{F}_q$, in particular we are interested in how many of them are reducible and in which form.

In particular, we recall some counts for curves of smaller degrees:

**Proposition 5.1.3.** *The number of irreducible conics over $\mathbb{F}_q$ is $q^5 - q^2$. The number of irreducible conics over $\mathbb{F}_{q^2}$ not defined over $\mathbb{F}_q$ is $q^{10} - q^5 - q^4 + q^2$. The number of irreducible cubics over $\mathbb{F}_q$ is $q^5(q+1)(q-1)(q^2+q+1)$.*

*Proof.* The first and the last results are discussed in [BCF15a]. The number of irreducible conics over $\mathbb{F}_{q^2}$ not defined over $\mathbb{F}_q$ can be computed using the first formula. Indeed, the total number of irreducible conics over $\mathbb{F}_{q^2}$ is $q^{10} - q^4$, minus the $q^5 - q^2$ that are defined over $\mathbb{F}_q$ we obtain the formula.

□

There are, up to scaling, $n_4 = \frac{q^{15}-1}{q-1}$ plane quartic curves. They can be either irreducible or a product of lower degree curves, such as lines $L_i$, irreducible conics $Q_l$ and irreducible cubics $C_k$ defined over $\mathbb{F}_q$ and its extensions. If not specified the curve is meant to be defined over the base field. By $\sigma_j$ we will refer to the Frobenius automorphism of $\mathrm{Gal}(\mathbb{F}_{q^j}/\mathbb{F}_q)$. We have the following possible factorizations:

(i) $L_1 \cdot L_2 \cdot L_3 \cdot L_4$ four $\mathbb{F}_q$-lines;

(ii) $L_1 \cdot L_2 \cdot L_3 \cdot \sigma_2(L_3)$ where $L_3$ and $\sigma_2(L_3)$ are conjugate lines over $\mathbb{F}_{q^2}$;

(iii) $L_1 \cdot \sigma_2(L_1) \cdot L_2 \cdot \sigma_2(L_2)$ where both $L_i$ are $\mathbb{F}_{q^2}$-lines which are not $\mathbb{F}_q$-rationals;

(iv) $L_1 \cdot L_2 \cdot \sigma_3(L_2) \cdot \sigma_3^2(L_2)$ where $L_2$ is defined over $\mathbb{F}_{q^3}$ but not $\mathbb{F}_q$;

(v) $L \cdot \sigma_4(L) \cdot \sigma_4^2(L) \cdot \sigma_4^3(L)$ where $L$ is defined over $\mathbb{F}_{q^4}$ but not $\mathbb{F}_{q^2}$;

(vi) $L_1 \cdot L_2 \cdot Q$;

(vii) $L \cdot \sigma_2(L) \cdot Q$ where $L$ is defined over $\mathbb{F}_{q^2}$ but not on $\mathbb{F}_q$;

(viii) $Q_1 \cdot Q_2$;

(ix) $Q \cdot \sigma_2(Q)$ where $Q$ defined over $\mathbb{F}_{q^2}$ but not $\mathbb{F}_q$;

(x) $L \cdot C$.

(xi) $T$ irreducible quartic

Let us count how many they are: in certain cases we split the computation in sub-cases. In the following lines the standard notation we use is that $L_i \neq L_j$ if and only if $i \neq j$:

(i) Total $(q^8 + 4q^7 + 16q^6 + 34q^5 + 66q^4 + 80q^3 + 85q^2 + 50q + 24)/24$

  (a) $\#\{T = L^4\} = n_1 = q^2 + q + 1$;

  (b) $\#\{T = L_1^3 \cdot L_2\} = n_1(n_1 - 1) = q(q + 1)(q^2 + q + 1)$;

  (c) $\#\{T = L_1^2 \cdot L_2 \cdot L_3\} = n_1(n_1-1)(n_1-2)/2 = q(q+1)(q^2+q+1)(q^2+q-1)/2$;

  (d) $\#\{T = L_1^2 \cdot L_2^2\} = n_1(n_1 - 1)/2 = q(q + 1)(q^2 + q + 1)/2$;

  (e) $\#\{T = L_1 \cdot L_2 \cdot L_3 \cdot L_4\} = n_1(n_1 - 1)(n_1 - 2)(n_1 - 3)/24 = q(q + 1)(q^2 + q + 1)(q^2 + q - 1)(q^2 + q - 2)/24$;

(ii) Total $(q^8 + 2q^7 + 4q^6 + 2q^5 - 4q^3 - 3q^2 - 2q)/4$

  (a) $\#\{T = L_1^2 \cdot L_2 \cdot \sigma(L_2)\} = n_1(n_1^{(2)} - n_1)/2 = q(q - 1)(q^2 + q + 1)^2/2$;

    - Without a quadruple point $(q^2)(n_1^{(2)} - n_1)/2 = q^3(q - 1)(q^2 + q + 1)$;
    - With a quadruple point $(q+1)(n_1^{(2)} - n_1)/2 = q(q-1)(q+1)(q^2+q+1)$;

  (b) $\#\{T = L_1 \cdot L_2 \cdot L_3 \cdot \sigma(L_3)\} = n_1(n_1-1)(n_1^{(2)}-n_1)/4 = q^2(q^2-1)(q^2+q+1)^2/4$;

(iii) Total $(q^8 - 2q^5 + 2q^4 + q^2 - 2q)/8$

  (a) $\#\{T = L_1 \cdot \sigma(L_1) \cdot L_2 \cdot \sigma(L_2)\} = (n_1^{(2)} - n_1)(n_1^{(2)} - n_1 - 2)/8 = q(q - 1)(q^2 + q + 1)(q^4 - q - 2)/8$;

    - Without a quadruple point $(q^4 - q)(q^2 - q)(q^2 + q)/8$;
    - With a quadruple point $(q^2 + q + 1)(q^2 - q)(q^2 - q - 2)/8$;

(b) $\#\{T = (L \cdot \sigma(L))^2\} = (n_1^{(2)} - n_1)/2 = q(q-1)(q^2+q+1)/2$;

(iv) $\#\{T = L_1 \cdot L_2 \cdot \sigma_3(L_2) \cdot \sigma_3^2(L_2)\} = (n_1^{(3)} - n_1)(n_1)/3 = (q-1)q(q+1)(q^3+q+1)(q^2+q+1)/3$;

(v) $\#\{T = L \cdot \sigma_4(L) \cdot \sigma_4^2(L) \cdot \sigma_4^3(L)\} = (n_1^{(4)} - n_1^{(2)})/4 = q^2(q^6-1)/4$;

(a) $\#\{T = L \cdot \sigma_4(L) \cdot \sigma_4^2(L) \cdot \sigma_4^3(L) | T \text{ has one quadruple point on } \mathbb{F}_q\} = n_1^{(2)} \frac{t_4^2 - t_2^2 - (t_4^1 - t_2^1)n_1^{(2)}}{4(t_4^1 - t_2^1)} = (q^2+q+1)\frac{q^4-q}{4}$;

(b) $\#\{T = L \cdot \sigma_4(L) \cdot \sigma_4^2(L) \cdot \sigma_4^3(L) | T \text{ has no point on } \mathbb{F}_q\} = \frac{q^8 - q^6 - q^5 - q^4 + q^3 + q}{4}$;

(vi) Total $(q^9 + 2q^8 + 4q^7 + 2q^6 - 4q^4 - 3q^3 - 2q^2)/2$

(a) $\#\{T = L_1 \cdot L_2 \cdot Q\} = n_1(n_1-1)(q^5-q^2)/2 = q^3(q-1)(q+1)(q^2+q+1)^2/2$;

(b) $\#\{T = L_1^2 \cdot Q\} = n_1(q^5-q^2) = (q^2+q+1)(q^5-q^2)$;

(vii) $\#\{T = L \cdot \sigma(L) \cdot Q\} = (n_1^{(2)} - n_1)(q^5-q^2)/2 = q^3(q-1)^2(q^2+q+1)^2/2$;

(viii) $\#\{T = Q_1 \cdot Q_2\} = (q^5-q^2)(q^5-q^2+1)/2$;

(a) $\#\{T = Q_1 \cdot Q_2\} = (q^5-q^2)(q^5-q^2-1)/2$ by Proposition 5.1.3;

(b) $\#\{T = Q^2\} = (q^5-q^2)$;

(ix) $\#\{T = Q \cdot \sigma(Q)\} = (q^{10} - q^5 - q^4 + q^2)/2$; by Proposition 5.1.3;

(x) $\#\{T = L \cdot C\} = q^5(q^2-1)n_1^2 = q^5(q^2-1)(q^2+q+1)^2$ by Proposition 5.1.3;.

Adding up all the cases above we obtain the total of reducible ones:

$$R = q^{11} + 3q^{10} + 3q^9 + 2q^8 + q^5 + q^4 + q^3 + q^2 + q + 1.$$

Therefore, the number of irreducible quartics over $\mathbb{F}_q$ is

$$n_4^{(1)} - R = q^{14} + q^{13} + q^{12} - 2q^{10} - 2q^9 - q^8 + q^7 + q^6. \tag{5.1}$$

## 5.2 Product of conjugate conics over $\mathbb{F}_{q^2}$

Although we have already computed the total number of product of conjugate conics over $\mathbb{F}_{q^2}$ the number of $\mathbb{F}_q$-rational points over these quartics may vary, therefore we need to partition them accordingly and count the cardinality of each subset. When

one conic has a $\mathbb{F}_q$-rational point $P$ then $P$ belongs to the conjugate curve as well, since it is fixed by the Galois action. Then all the $\mathbb{F}_q$-rational points are contained in the intersection between the two curves which, by Bézout's Theorem, has cardinality 4 containing multiplicities. Since the reduction of a $\mathbb{Q}_q$-rational point on a quartic over $\mathbb{Z}_q$ must be $\mathbb{F}_q$ rational, we partition the quartics by the number of points defined over $\mathbb{F}_q$ and their multiplicities. Later on we will use these counts to evaluate the probability of solubility of a quartic whose reduction is a union of two conjugate conics.

In the following Table 5.1 we list all the polynomials describing the cardinality of the associated subsets, the first column indicates the number of $\mathbb{F}_q$ points, the second the intersection multiplicities associated to each point (which we will use later as label for each case since this "vector" determines uniquely the associated partition of conjugate conics), the third the cardinality.

| $\#\gamma \cap \overline{\gamma}(\mathbb{F}_q)$ | $I_P(\gamma, \overline{\gamma})$ | Cardinality |
|---|---|---|
| 0 | 0 | $(3q^{10} - 3q^9 - 3q^8 - 4q^7 + 7q^6 + 3q^5 + q^4 - 4q^3)/16$ |
| 1 | 1 | $(q^{10} - q^9 - q^8 + q^6 + q^5 - q^4)/6$ |
| 1 | 2 | $(q^9 - q^7 - q^6 + q^4)/4$ |
| 1 | 4 | $(q^7 - q^5 - q^4 + q^2)/2$ |
| 2 | 1,1 | $(q^{10} - q^9 - 3q^8 + 3q^6 + 3q^5 - q^4 - 2q^3)/8$ |
| 2 | 2,2 | $(q^8 + q^7 - q^5 - q^4)/4$ |
| 2 | 1,3 | $(q^8 - q^6 - q^5 + q^3)/2$ |
| 3 | 1,1,2 | $(q^9 - q^7 - q^6 + q^4)/4$ |
| 4 | 1,1,1,1 | $(q^{10} - q^9 - q^8 + q^6 + q^5 - q^4)/48$ |

Table 5.1: Conjugate conics cardinalities

We want to gain information from the geometric conditions we have on the intersection points and express them in terms of the arithmetic of the polynomials describing the locus of the quartics. Let us consider a $\mathbb{F}_q$-rational intersection point $P$, if its intersection multiplicity between the two conjugate curves is one it means that the tangent lines at $P$ of each curve are distinct; then, since these lines are conjugate, we have that the tangent lines are defined over $\mathbb{F}_{q^2}$ but not over $\mathbb{F}_q$. If we have a point $P$ of multiplicity at least two the conics have the same tangent line at $P$ which implies that the tangent line is defined over $\mathbb{F}_q$ (up to scaling by an element of $\mathbb{F}_{q^2}$). Therefore, we can move the point $P$ to $[1:0:0]$ and the line to $y = 0$ and write the product of the two conjugate conics as

$$\gamma\overline{\gamma} = (xy + Q(y,z))(xy + \overline{Q}(y,z)),$$

where $Q(y,z)$ is a binary quadratic form defined over $\mathbb{F}_{q^2}$ but not on $\mathbb{F}_q$ (as said above the tangent line is $\mathbb{F}_q$-rational up to multiplication by a coefficient in $\mathbb{F}_{q^2}$, we can divide the quartics by the norm of this coefficient, in this way the coefficient of $xy$ is 1). In this case we can use the properties of the intersection multiplicity to understand what constraints we have on $Q(y,z)$. De-homogenizing with respect to $x$, we have

$$I_{(0,0)}(\gamma,\overline{\gamma}) = I_{(0,0)}(y+Q, Q-\overline{Q}) = I_{(0,0)}(y+Q, L_1L_2) = \sum_{i=1}^{2} I_{(0,0)}(y+Q, L_i),$$

where $Q-\overline{Q} = L_1L_2$ over $\mathbb{F}_{q^2}$ since up to scaling $Q-\overline{Q}$ is defined over $\mathbb{F}_q$. We have that $I_{(0,0)}(y+Q, L_i)$ is 2 if $y|L_i$ (i.e. $L_i$ is tangent at $y+Q$ in $(0,0)$) or 1 otherwise. So we have that the intersection multiplicity is 2 if $y \not| Q-\overline{Q}$, 3 if $y|Q-\overline{Q}$ but $y^2 \not| Q-\overline{Q}$ and 4 if $y^2|Q-\overline{Q}$. Now we explain briefly each count: for each subset we find a standard model which we use in a following section to compute the probabilities of solubility, we refer to the vector of multiplicities intersection as $m$.

For $m=0$ we can compute the difference between the total of reductions which factor in a product of two conjugate conics computed in Section 5.1 and the sum of all the other quantities computed here.

In the first two cases, $m=1$ and $m=1,1$, writing the condition on the conic does not guarantee its irreducibility, indeed it may factor as a product of two lines (not conjugate) defined over $\mathbb{F}_{q^2}$.

For $m=1$ we need first to compute how many quartics have at least one point with multiplicity one. Once we fix the singular point we have $\gamma = xy+\alpha xz+\beta y^2+\delta yz+\epsilon z^2$, with $\alpha$ in $\mathbb{F}_{q^2}\setminus\mathbb{F}_q$, $\beta,\delta$ and $\epsilon$ in $\mathbb{F}_{q^2}$. We need to eliminate from the count the reducible ones, which are unions of two non conjugate $\mathbb{F}_{q^2}$-lines, they cannot be two $\mathbb{F}_{q^4}$ lines because it would imply either $m=4$ or $m=0$. Assuming the characteristic to be greater than 2, since the determinant associated to the conic above is $2\delta\alpha-2\alpha^2\beta-2\epsilon$ and $\alpha$ is not zero, we have that $\delta=\alpha^2\beta+\epsilon/\alpha$ if and only if the conic is irreducible. Therefore, we have $q^2-1$ choices for $\delta$. In characteristic equal to two we can count the irreducible ones by difference with the reducible ones and obtain the same count in function of $q$.

For $m=1,1$ we need first to compute how many quartics have at least two points both with multiplicity one. Once one fixes the two points we have $\gamma = xy+\alpha xz+\beta yz+\gamma z^2$, with $\alpha$ in $\mathbb{F}_{q^2}\setminus\mathbb{F}_q$, $\beta$ and $\delta$ in $\mathbb{F}_{q^2}$. We need to eliminate from the count the reducible ones, which are unions of two non conjugate $\mathbb{F}_{q^2}$-lines. Since the determinant associated to the conic above is $\alpha\beta-\gamma$ and $\alpha$ is not zero, we have that $\beta=\gamma/\alpha$ if and only if the conic is irreducible. Therefore, we have $q^2-1$ choices for $\beta$. Then we can compute

the difference between the number of these models and the ones with $m = 1, 1, 2$ and $m = 1, 1, 1, 1$ with the first two points fixed, in order to calculate the number of quartics with exactly two singular $\mathbb{F}_q$-rational points of multiplicity one.

For $m = 2$ we proceed in a similar way as for $m = 1$: we first find a model with at least one point of multiplicity 2 and then subtract the counts for $m = 2, 2$ and $m = 1, 2, 2$. Fixing the point and the line then the model is $\gamma = (xy + \alpha y^2 + \beta yz + \delta z^2)$, with $\alpha, \beta \in \mathbb{F}_{q^2}$ and $\delta$ in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ (which guarantees that the conic is irreducible and that the intersection multiplicity is 2).

For $m = 4$ we fix the singular point at $[1 : 0 : 0]$ and the tangent line to be $y = 0$, so we have that $Q - \overline{Q} = \alpha y^2$, then the coefficient of $yz$ and $z^2$ in $Q$ are $\mathbb{F}_q$-rational and the latter is not null. Then, to get the total we let the point and the tangent vary.

For $m = 2, 2$ fixing the two singular points and the intersection between the two tangent lines ($q^2$ choices since it cannot be aligned with the other two points) the model would be $(xy + \alpha z^2)(xy + \overline{\alpha} z^2)$ with $\alpha$ in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

For $m = 1, 3$ fixing the two points and the tangent line of the point of multiplicity 3 ($q$ choices for this one since it cannot pass through the other point) we have the reduction $(xy + \alpha xz + cz^2)(xy + \overline{\alpha} xz + cz^2)$, where $\alpha$ is in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $c \in \mathbb{F}_q^*$.

For $m = 1, 1, 2$ after we fix the three points we have two parameters for the pencils of conics: $q - 1$ to determine one of two irreducible conics in the pencil by fixing the line through the point of multiplicity 2 (but not containing the other two points) and $(q^2 - q)/2$ for the parameter of the pencil itself.

For $m = 1, 1, 1, 1$ once one fixes the 4 points then the pencil of conics is determined, the pencil has $(q^2 - q)/2$ pairs of conjugate conics.

An exhaustive search has been done to double-check the formulas for small primes.

## 5.3 Quartic polynomials and binary quartics forms over $\mathbb{F}_q$

Later on we will need the probabilities related to the roots of quartic polynomials and quartic binary forms. We describe them here

**Lemma 5.3.1.** *Of the $q^4$ monic quartics in $\mathbb{F}_q[X]$ we have:*

- *Among the $q^4 - q^3$ which have distinct roots there are:*
  - $\frac{q(q-1)(q-2)(q-3)}{24}$ *with distinct roots in $\mathbb{F}_q$.*
  - $\frac{q^2(q-1)^2}{4}$ *with 2 distinct roots in $\mathbb{F}_q$ and two conjugate in $\mathbb{F}_{q^2}$.*
  - $\frac{(q^2-q)(q^2-q-2)}{8}$ *with two distinct pairs of conjugate roots in $\mathbb{F}_{q^2}$.*

  - $\frac{q^4-q^2}{3}$ *with one in* $\mathbb{F}_q$*, three conjugate roots in* $\mathbb{F}_{q^3}$.
  - *with* $\frac{q^4-q^2}{4}$ *four conjugate roots in* $\mathbb{F}_{q^4}$.

- *Among the* $q^3 - 2q^2 + q$ *which have two distinct roots and a double one there are:*
  - $\frac{q(q-1)(q-2)}{2}$ *with all roots in* $\mathbb{F}_q$.
  - $\frac{q(q^2-q)}{2}$*, with the double root in* $\mathbb{F}_q$ *and the conjugate roots in* $\mathbb{F}_{q^2}$.

- *Among the* $q^2 - q$ *which have two double roots there are:*
  - $\frac{q(q-1)}{2}$ *with the roots in* $\mathbb{F}_q$.
  - $\frac{q^2-q}{2}$ *with the roots in* $\mathbb{F}_{q^2}$.

- $q(q-1)$ *have a triple root and a distinct root in* $\mathbb{F}_q$.

- $q$ *have a quadruple root in* $\mathbb{F}_q$.

By the previous Lemma we can compute the probabilities of having solubility, insolubility or being in an undetermined case when we have a monic quartic as reduction.

**Corollary 5.3.2.** *The probability that a random monic quartic over* $\mathbb{F}_q$ *has a simple root in* $\mathbb{F}_q$ *is* $\sigma_1 = \frac{5q^3-2q^2-q-2}{8q^3}$*, and the probability that it has a quadruple root is* $\tau_1 = \frac{1}{q^3}$*. Then the probability that it has just one double root on* $\mathbb{F}_q$ *but no simple ones is* $\rho_1 = \frac{q-1}{2q^2}$*. The probability of having two double roots in* $\mathbb{F}_q$ *is* $\theta_1 = \frac{q-1}{2q^3}$*. The remaining cases, which have no roots in* $\mathbb{F}_q$*, have probability* $\frac{3q^3-2q^2+q-2}{8q^3}$.

Similarly, we make the same count for the binary quartics.

**Lemma 5.3.3.** *Of the* $q^5$ *binary quartics in* $\mathbb{F}_q[X, Y]$ *we have:*

- *Among the* $q^5 - q^4 - q^3 + q^2$ *which have distinct roots there are:*
  - $\frac{(q+1)q(q-1)(q-2)(q-1)}{24}$ *with distinct roots in* $\mathbb{F}_q$.
  - $\frac{(q+1)q^2(q-1)^2}{4}$ *have 2 with distinct roots in* $\mathbb{F}_q$ *and two conjugate in* $\mathbb{F}_{q^2}$.
  - $\frac{(q-1)(q^2-q)(q^2-q-2)}{8}$ *with two distinct pairs of conjugate roots in* $\mathbb{F}_{q^2}$.
  - $\frac{(q^3-q)(q+1)(q-1)}{3}$ *one over* $\mathbb{F}_q$*, with three conjugate in* $\mathbb{F}_{q^3}$.
  - $\frac{(q-1)(q^4-q^2)}{4}$ *with four conjugate in* $\mathbb{F}_{q^4}$.

- *Among the* $q^4 - q^3 - q^2 + q$ *which have two distinct roots and a double one there are:*

  - $\frac{(q+1)q(q-1)(q-1)}{2}$ *with all the roots in* $\mathbb{F}_q$.
  - $\frac{(q+1)(q-1)(q^2-q)}{2}$, *with the double root in* $\mathbb{F}_q$ *and the conjugate root in* $\mathbb{F}_{q^2}$.

- *Among the* $q^3 - q^2$ *which have two double roots there are:*
  - $\frac{(q+1)q(q-1)}{2}$ *with all the roots in* $\mathbb{F}_q$.
  - $\frac{(q-1)(q^2-q)}{2}$ *with all the roots in* $\mathbb{F}_{q^2}$.
- $(q+1)q(q-1)$ *have a triple root and a distinct one in* $\mathbb{F}_q$.
- $q^2 - 1$ *have a quadruple root in* $\mathbb{F}_q$.
- *1 is the zero form.*

**Corollary 5.3.4.** *The probability that a random binary quartic form over* $\mathbb{F}_q$ *has a simple root in* $\mathbb{P}^2(\mathbb{F}_q)$ *is* $\sigma = \frac{5q^4+q^3-3q^2-q-2}{8q^4}$, *and the probability that it has a quadruple root is* $\tau = \frac{q^2-1}{q^5}$. *Then the probability that it has just a double root in* $\mathbb{F}_q$ *but no simple ones is* $\rho = \frac{q^3-q^2-q+1}{2q^4}$. *With probability* $\theta = \frac{q^2-1}{2q^4}$ *it has 2 double roots in* $\mathbb{F}_q$. *With probability* $\frac{1}{q^5}$ *we have the zero form. The remaining cases, which have no roots in* $\mathbb{F}_q$, *have probability* $\frac{3q^4-5q^3+3q^2-3q+2}{8q^4}$.

## 5.4 Counting irreducible quartics

In this section we compute the polynomials describing the number of irreducible quartics $T$ classified by singularities that are defined in $\mathbb{P}^2(\mathbb{F}_q)$. The plane quartics are curves of genus 3, therefore we can have different types of irreducible curves: they may have one, two or three double points, or just one triple point, or are smooth curves. Usually we will denote by $f$ as polynomial associated to $T$. The general approach to computing the different irreducible quartics is as follows:

(i) consider a specific type of singularity (by number of points and multiplicity);

(ii) consider a specific field of definition for the singular points;

(iii) fix, if possible, by a change of coordinates, the singular points;

(iv) deduce the algebraic conditions on the coefficients of $f$ to characterize the singularity at the fixed points;

(v) between the $f$'s satisfying the conditions above count how many are reducible/irreducible polynomials;

(vi) multiply the number of irreducible ones by the number of possible positions of the singularities.

This method works well with most of the cases but in certain cases it is complicated to determine the multiplicative factor at step (vi) or to have enough conditions to work out exactly the number of irreducible ones at step(v). We may have to split our counting into several sub-cases and then proceed using the inclusion-exclusion principle. Unfortunately in some cases, when we have just one or two $\mathbb{F}_q$-rational singular points, the number of subcases rises a lot and therefore we decided to use another method. Indeed, in the most intricate cases we proceed with an exhaustive count of the number of quartics defined over $\mathbb{F}_q$ for small $q$ satisfying the required conditions and then, once we have these values, we interpolated them to obtain a polynomial formula in $q$.

We find by direct computation the polynomial that describes the number of irreducible quartics in $\mathbb{P}^2(\mathbb{F}_q)$ having a triple singular point, two conjugate points over $\mathbb{F}_{q^2}$ or three singular points. In particular, in the latter case we specialise the computation by the different fields of definition of the singular points: indeed, they can either be all defined over $\mathbb{F}_q$, two conjugate ones over $\mathbb{F}_{q^2}$ and one over $\mathbb{F}_q$ or three conjugate points over $\mathbb{F}_{q^3}$. What is left are just the curves with one or two singular double points defined over $\mathbb{F}_q$. Thanks to a routine written in Sage [Sag18], which gives us the exact count for small fields, we are able, by interpolation, to compute the polynomials in $q$ describing the cardinalities of such curves for each finite field.

The fact that all the counts considered are polynomials, and therefore we can interpolate to work out the missing cases, can be explained as follows. These counts are described by functions from the set of prime powers to the non-negative integers. Each count depends just on the cardinality of the base field and there are no differences related to the fact that for small $q$ the plane $\mathbb{P}^2(\mathbb{F}_q)$ has few elements, which means that we never encounter the situation where there are not enough points or lines in the plane. Therefore, fixing the case we want to investigate, the count would be described by a unique function (not piecewise defined) whose argument is just the cardinality of the field. Assuming that this function $t$ is rational we see that it actually is a polynomial. Indeed, by polynomial division, we can write $t$ as sum of a polynomial $f$ and a rational function $r$, which the degree of denominator is greater than that of the numerator. By the fact that $t$ and $f$ images are contained in $\mathbb{Z}$, the same is true for the image of $r$. If we consider the limit of $r$, for $q \to \infty$, we would get 0, but since $r$ assumes just integer values this can happen if and only if $r$ is identically zero by continuity. Therefore $t = f$, and is a polynomial.

### 5.4.1 Three singular points

The maximum number of singular points an irreducible quartic $T$ can have is three. In this case the singular points which must have multiplicity 2 can be defined over different fields, indeed they can be either all defined over $\mathbb{F}_q$, two conjugate ones over $\mathbb{F}_{q^2}$ and one over $\mathbb{F}_q$ or three conjugate points over $\mathbb{F}_{q^3}$. In this section we count for each of the three configurations the number of such curves over $\mathbb{P}^2(\mathbb{F}_q)$.

**Proposition 5.4.1** (Three double points defined over $\mathbb{F}_q$)**.** *The number of irreducible quartics in $\mathbb{P}^2(\mathbb{F}_q)$ having three singular points defined over $\mathbb{F}_q$ is*

$$\frac{q^{11}-q^{10}-q^9-q^8+q^7+2q^6-q^3}{6}. \tag{5.2}$$

*Proof.* We change the coordinates in order to map the 3 singular points to the basic triangle of $\mathbb{P}^2(\mathbb{F}_q)$ since they are not collinear. Indeed, if they were collinear the line passing through them would have 6 intersections (counting multiplicities) with $T$ and therefore, by Bézout's Theorem, $T$ would contain the line itself and so it would be reducible. The possible configurations of the three double points are $(q^2+q+1)(q^2+q)q^2/6$.

After the change of coordinates $f$, the associated polynomial to $\overline{T}$, has no terms in $x^4, x^3y, x^3z, y^4, y^3x, y^3z, z^4, z^3x, z^3y$, therefore we can rewrite it as

$$f = x^2(a_1y^2+a_2yz+a_3z^2)+x(a_4y^2z+a_5yz^2)+a_6y^2z^2 = x^2C_2(y,z)+xC_3(y,z)+C_4(y,z),$$

where $C_i$ are forms of degree $i$. Notice that if $a_6 = 0$ then $x|f$, therefore $T$ would be reducible. With similar argument we conclude that $a_1, a_3$ and $a_6$ are all non-zero.

$C_2(y,z)$ is a product of the two lines, which may be defined over $\mathbb{F}_{q^2}$, tangent to $T$ in $[1:0:0]$, $C_3(y,z)$ is the product of three lines ($y=0, z=0$ and $a_4y+a_5z=0$) and $C_4(y,z)$ is the product of two double lines ($y=0$ and $z=0$). Therefore, the only common factors of the forms $C_i$ could be $y$ and/or $z$ but, imposing $a_1 \neq 0 \neq a_3$, we have already avoided this possibility.

Hence, if $f$ is reducible, both factors will have a linear term in $x$, so $f$ splits as two quadratic factors or as a linear one times a cubic. Let us study the latter case first: we can then write $f$ as $(x+L)(xC_2+C)$, where $L$ and $C$ are respectively a linear and cubic term in $y$ and $z$. This would imply $C_3 = LC_2 + C, C_4 = LC$ therefore $y$ or $z$ would divide $L$, but $C_2$ has both terms in $y^2$ and $z^2$ since $a_1 \neq 0 \neq a_3$ and so $LC_2$ would have a term either in $y^3$ or $z^3$, which is a contradiction.

It remains to study the product of two conics: $f$ would have the following form

$$f = (xL_1 + \alpha)(xL_2 + \beta),$$

where $L_1L_2 = C_2$ and $\alpha\beta = C_4$. In order to avoid terms in $y^3$ and $z^3$ in $C_3$, the two conics $\alpha$ and $\beta$ must be $yz = 0$, here we scale them in order to have both the coefficients of $yz$ equal to 1 and $a_6 = 1$. Summing up, if $f$ is reducible it can be just in this form

$$f = \big(x(r_1y + s_1z) + yz\big)\big(x(r_2y + s_2z) + yz\big)$$

where $r_i \neq 0 \neq s_i$ (otherwise either $a_1$ or $a_3$ would be equal to zero). We can then count the total of reducible cases, notice that the factorisation can happen over $\mathbb{F}_q$ or $\mathbb{F}_{q^2}$. We have $(q-1)^2$ choices for $L_i = r_iy + s_iz$ defined over $\mathbb{F}_q$ and therefore we have $(q-1)^2((q-1)^2+1)/2$ choices over $\mathbb{F}_q$. On $\mathbb{F}_{q^2}$ we have $((q^2-1)^2 - (q-1)^2)/2$ choices, which makes a total of $q^4 - 2q^3 + 2q^2 - 2q + 1$ possible ways to factor $f$. By the condition imposed ($a_6 = 1, a_1 \neq 0 \neq a_3$) the total number of possible $f$ is $q^3(q-1)^2$. Therefore, by computing the difference with the reducible ones we have $q^5 - 3q^4 + 3q^3 - 2q^2 + 2q - 1$ irreducible quartics, times $(q^2+q+1)(q^2+q)q^2/6$ we have a total of $\frac{q^{11}-q^{10}-q^9-q^8+q^7+2q^6-q^3}{6}$ irreducible quartics with 3 double points defined over $\mathbb{F}_q$, up to scaling. □

**Proposition 5.4.2** (One point over $\mathbb{F}_q$ and two points conjugate over $\mathbb{F}_{q^2}$ )**.** *The number of irreducible quartics in $\mathbb{P}^2(\mathbb{F}_q)$ having one point over $\mathbb{F}_q$ and two points conjugate over $\mathbb{F}_{q^2}$ is*

$$\frac{q^{11} - q^{10} - q^9 + q^8 + q^7 - 2q^5 + q^3}{2}. \tag{5.3}$$

*Proof.* As first step we notice that the line passing through the two conjugate singular points cannot pass through the third singular one as well, otherwise $T$ would not be irreducible, by Bézout's Theorem. Moreover, this line is defined over $\mathbb{F}_q$ since it is fixed under the Galois action. We can move the double point defined over $\mathbb{F}_q$ to $[0:0:1]$ and the line to $z = 0$, so we have $t_1$ possibilities for the point and $n_1 - (q+1) = q^2$ for the line. So the polynomial $f$ associated to $T$ would be $f = z^2C_2 + zC_3 + \alpha^2$, where $\alpha$ is a quadratic form in $x$ and $y$ irreducible over $\mathbb{F}_q$ but reducible over $\mathbb{F}_{q^2}$. The form of $\alpha$ is due to the fact that the intersection between $T$ and the line $z = 0$ is the two conjugate singular points. As in the previous section, to force the singularity in the two conjugate points, we need $\alpha | C_3$, which will lead to the equation:

$$f = z^2C_2 + z\alpha C_1 + \alpha^2$$

Notice that $f$ would be reducible if $\alpha$ divides $C_2$ or if it splits in two quadratic factors, both linear in $z$. The possible factorisations of $\alpha^2$ can be: either $\alpha \cdot \alpha$ or $(x - ty)^2 \cdot (x - \sigma(t)y)^2$. It follows that we have 3 sub-cases, then, by inclusion-exclusion, we will work out the total number of reducible ones.

(i) $\alpha | C_2 \iff C_2 = \alpha C_0$ so we have $q^2$ choices for $C_1$ and $q-1$ for $C_0$ which makes a total of $q^3 - q^2$.

(ii) $f = (Lz + \alpha)(L'z + \alpha)$, where $LL' = C_2$ over $\mathbb{F}_{q^2}$. Notice that we have $C_3 = \alpha(L + L')$. So we just need to count the choices for $L$ and $L'$: if they are defined over $\mathbb{F}_q$ we obtain $(q^2-1)(q^2)/2$ choices, otherwise, if they are defined over $\mathbb{F}_{q^2}$, we obtain $(q^4 - q^2)/2$ choices, which makes a total of $q^4 - q^2$.

(iii) $f = (Lz+t^2)(\sigma(L)z+\sigma(t)^2)$. In this case we have $\sigma(L)t^2+L\sigma(t)^2 = C_1\alpha = C_1 t\sigma(t)$, which implies $t|L$, and so $\alpha|C_2$. Therefore this case is actually a sub-case of (i).

Then we just need to subtract the counts for the curves in $(i) \cap (ii)$; this case occurs just when $\alpha | LL'$, so for $q^2 - 1$ (which correspond to only one choice for $L$ up to coefficient). Therefore we have $q^4 + q^3 - 3q^2 + 1$ reducible quartics. The total is $q^2(q^3-1) = q^5 - q^2$ so the irreducible ones are $q^5 - q^4 - q^3 + 2q^2 - 1$ times the choices we made, so $t_1$ for the point, $q^2$ for the line and the number of possible $\alpha$, that is a product of two conjugate linear equation in $x$ and $y$ over $\mathbb{F}_{q^2}$, is $(q^2 - q)/2$. Then we have a total of $\frac{q^{11}-q^{10}-q^9+q^8+q^7-2q^5+q^3}{2}$ irreducible quartics with three double points, which two of them conjugate over $\mathbb{F}_{q^2}$. □

**Proposition 5.4.3** (Three points conjugate over $\mathbb{F}_{q^3}$)**.** *The number of irreducible quartics in $\mathbb{P}^2(\mathbb{F}_q)$ having three points conjugate over $\mathbb{F}_{q^3}$ is*

$$\frac{q^{11} - q^{10} - q^9 - q^8 + q^7 + 2q^6 - q^3}{3}. \tag{5.4}$$

*Proof.* If the irreducible quartic $T$ has three double points conjugate over $\mathbb{F}_{q^3}$ they cannot be collinear, indeed if we consider the line passing throw them it will have 6 intersection with T (counting multiplicities) and therefore will be itself part of the quartic, making it reducible.

As usual, to count the irreducible ones, we will subtract the number of reducible ones from the total. Before let us count the number of *triangles* whose vertices are 3

conjugate points over $\mathbb{F}_{q^3}$, not collinear. We have $(t_3 - t_1)/3$ orbits with cardinality 3 in $\mathbb{P}^2\mathbb{F}_{q^3}$). If an orbit lies in a line then the line is fixed under the Galois action and so is defined over $\mathbb{F}_q$. For each of the $n_1$ lines defined over $\mathbb{F}_q$ we have $(t_3^{(1)} - t_1^{(1)})/3$ orbits with cardinality 3 on it. Therefore, the total number of triangles is

$$\frac{(t_3 - t_1)}{3} - n_1 \frac{(t_3^{(1)} - t_1^{(1)})}{3} = \frac{q^6 - q^5 - q^4 + q^3}{3}$$

Now, the total number of quartics defined over $\mathbb{F}_q$ having a *singular triangle* is $(q^6 - 1)/(q - 1)$. Indeed, we need to impose 9 linear independent conditions on the 15 coefficients to force the quartics to have a specific singular triangle. Notice that the number of independent equations is just 9 thanks to the Euler's Homogeneous Function Theorem, indeed it provides the linear relation

$$x\frac{\partial f}{\partial x} + y\frac{\partial f}{\partial y} + z\frac{\partial f}{\partial z} = 4f$$

where the zero locus of $f$ is the quartic $T$. Notice that when $\mathrm{char}(\mathbb{F}_q) = 2$ we still have 9 independent equations since the derivatives are dependent.

Given this configuration of singular points, which quartics are reducible? We can have the 3 conjugate lines passing through these 3 points times a line defined over $\mathbb{F}_q$. So in this case we have $n_1 = t_1$ quartics per triangle.

Then we can have a product of two conics whose intersection consists of the triangle and a fourth $\mathbb{F}_q$-point. To force a conic passing through 4 points we intersect the general equation with 6 coefficients with 4 linear equations, scaling the result we have just one degree of freedom. Therefore, if we pick two conics passing through the 4 points their linear combinations will describe the entire pencil of conics. If the conics are defined over $\mathbb{F}_q$ there are $q+1$ conics in the pencil, $q^2+1$ over $\mathbb{F}_{q^2}$. If follows we have $(q+1)q/2$ couples of distinct conics defined on $\mathbb{F}_q$ passing through the 4 points, $(q^2 - q)/2$ couples of conjugate conic $\mathbb{F}_{q^2}$. We need to be bit a more careful with the $q+1$ squared conics: they will have $q+1$ double $\mathbb{F}_q$ points on them, so to avoid double counting we just add $(q+1)/(q+1) = 1$ squared conic. In total, we have $q^2+1$ quartics made by two conics per point and per triangle, so $(q^2+1)t_1$ quartics per triangle.

Therefore, for each triangle we have $t_1(q^2+2)q^4 + q^3 + 3q^2 + 2q + 2$ reducible quartics.

The number of irreducible quartics per triangle is $(q^6 - 1)/(q - 1) - (q^4 + 2q^3 + 4q^2 + 3q + 2) = q^5 - 2q^2 - q - 1$. In conclusion, we have $\frac{q^{11} - q^{10} - q^9 - q^8 + q^7 + 2q^6 - q^3}{3}$ irreducible quartics with three conjugate over $\mathbb{F}_{q^3}$ singular points. □

### 5.4.2 One triple point

In this case we have just one singular point with multiplicity 3. Later on we will focus on the smooth points contained in these curves over $\mathbb{F}_q$, in this particular case we have always a smooth point by Bézout's Theorem: if we consider a $\mathbb{F}_q$-rational line through the singular point that is not tangent to $T$ then the line intersects $T$ in another point with multiplicity 1, and so it is non-singular. Since the number of $\mathbb{F}_q$-rational tangent at the triple points is at most 3 we have at least $q+1-3$ such lines and so $q-2$ smooth points over the irreducible curve. Therefore, if $q \geq 3$, the irreducible curve with a triple point has at least a smooth point. For curves defined over $\mathbb{F}_2$ this is not true in general, indeed the curve

$$T : xy^2z + xyz^2 + y^4 + y^3z + z^4 = 0$$

is irreducible with a triple point in $[1:0:0]$ but has no smooth points.

**Proposition 5.4.4.** *The number of irreducible quartics in $\mathbb{P}^2(\mathbb{F}_q)$ having one triple point is*

$$q^{10} + q^9 - q^7 - q^6.$$

*Proof.* If we have just one singular point it has to be defined over $\mathbb{F}_q$, since it is stable under the Galois action. Fix the triple point to be $P_2 = [0:0:1]$. We distinguish the cases by the tangents to the curve at the point. In particular, the tangents are just the factors of the binary cubic in $x$ and $y$ in the equation of $T$.

(i) A triple line $L$, therefore we have

$$f = L^3z + C_4(x,y),$$

where $C_4$ is a degree 4 homogeneous polynomial. For $T$ to be irreducible we need $L$ to not divide $C_4$, so we have $q+1$ choices for $L$ times $q^5 - q^4$ for the quartic polynomial, so in total $q^6 - q^4$.

(ii) A double line $L$ and a line $L'$

$$f = L^2L'z + C_4(x,y),$$

again we just need to avoid $L$ or $L'$ to divide $C_4$. We have $q(q+1)$ choices for the two lines and $q^5 - 2q^4 + q^3$ for $C_4$.

(iii) Three distinct lines $L_i$,

$$f = L_1 L_2 L_3 z + C_4(x, y),$$

we need to split further in 3 cases by the definition field of the lines.

(a) All the lines defined over $\mathbb{F}_q$: we have $(q+1)q(q-1)/6$ choices for the lines and $q^5 - 3q^4 + 3q^3 - q^2$ choices for $C_4$ by inclusion-exclusion.

(b) Two lines conjugate over $\mathbb{F}_{q^2}$ and one over $\mathbb{F}_q$: we have $(q^2-q)/2$ choices for the conjugate lines, $q+1$ for the one defined over $\mathbb{F}_q$ and $q^5 - q^4 - q^3 + q^2$ for $C_4$.

(c) Three lines conjugate over $\mathbb{F}_{q^3}$: we have $(q^3-q)/3$ choices for the conjugate lines and $q^5 - q^2$ for $C_4$.

Adding up we obtain $q^8 - q^6$ irreducible quartics with a triple singular point in $[0:0:1]$. Counting the $t_1$ possible positions of the singular point, we have a total of $q^{10}+q^9-q^7-q^6$ irreducible quartics with a triple singular point up to scaling. □

### 5.4.3 Two double points conjugate over $\mathbb{F}_{q^2}$

**Proposition 5.4.5.** *The number of irreducible quartics in $\mathbb{P}^2(\mathbb{F}_q)$ having at least two double points conjugate over $\mathbb{F}_q^2$ is*

$$\frac{q^{12} - q^{10} - q^9 + q^7}{2}. \tag{5.5}$$

*Proof.* Let us consider the line through the two conjugate points over $\mathbb{F}_q^2$. Since it is invariant under the Galois action it is defined over $\mathbb{F}_q$, we fix it as $z = 0$. When we intersect the line $z = 0$ and the equation of $T$ we will obtain a quartic equation in $x$ and $y$, assuming $T$ irreducible the line $z = 0$ cannot intersect $T$ in points other than the two singular ones. Notice that the $y$ coordinates of the two singular points have to be non-zero, otherwise they would coincide. Therefore, dehomogenizing the equation with respect to $y$, we have a quartic univariate polynomial with two conjugate double roots, which are the ratios of the $x$ and $y$ coordinates of the two singular points. The quartic in $x$ and $y$ is a product of two conjugate lines over $\mathbb{F}_{q^2}$ squared, we will refer to it as $\alpha^2$, where $\alpha = (x - ty)(x + \sigma(t)y)$ with $P = [t : 1 : 0]$ and $\sigma(P) = [\sigma(t) : 1 : 0]$ the two singular points. Then, the equation $f$ of $T$ will be $C_0 z^4 + C_1 z^3 + C_2 z^2 + C_3 z + \alpha^2 = 0$. Unfortunately this does not imply that $P$ and $\sigma(P)$ are singular. The Jacobian of $f$ at $P$ or $\sigma(P)$ is null if and only if $\alpha | C_3$, therefore the equation $f$ we want to study is:

$$T : C_0 z^4 + C_1 z^3 + C_2 z^2 + C_1' \alpha z + \alpha^2 = 0.$$

A common factor between the $C_i$ forms would be possible if and only if $C_0 = 0 = C_1$, since $\alpha$ is irreducible over $\mathbb{F}_q$. This would imply that $[0:0:1]$ is a double point, and we have already counted this case in Section 5.4.2.

If $C_0 = 0$ and $C_1 \neq 0$ the only possible factorisation, thanks to Galois invariance, would be a quadratic term in $z$ times a linear one:

$$(z^2 D_0 + z D_1 + \alpha)(z E_1 + \alpha),$$

where we have, since $C_1 \neq 0$, $q-1$ choices for $D_0$ and $q^2-1$ for $E_1$ and $q^2$ for $D_1$. Knowing that in total there are $q^7 - q^5$ such quartics, the irreducible ones are $q^7 - 2q^5 + q^4 + q^3 - q^2$.

If $C_0 \neq 0$ again, by the Galois invariants, the quartics could factor just as a product of two conics. According to how $\alpha^2$ factorises in the two conics we have a different count: it can factor as $\alpha \cdot \alpha$ or as $(x - ty)^2 \cdot (x - \sigma(t)y)^2$, where the singular point is $[t:1:0]$. In the first case we will have

$$(z^2 D_0 + z D_1 + \alpha)(z^2 E_0 + z E_1 + \alpha),$$

where, as usual, $D_i$ and $E_i$ are homogeneous polynomials of degree $i$ in $x$ and $y$. The count of $D_i$ and $E_i$ depends on their field of definition, which could be $\mathbb{F}_q$ or $\mathbb{F}_q^2$, counting all 4 possible cases we have:

$$\frac{(q-1)q^2(1 + (q-1)q^2 - 1) + (q^2 - q)(q^4 - q^2) + (q-1)(q^4 - q^2) + q^2(q-q)}{2}.$$

We have intersection between the factorisations described above when $f$ factors in 4 distinct factors conjugate in pairs, which give us $(q^2-1)(q^2-2)/2$ quartics. Hence, the number of reducibles in this case is $\frac{q^7 - 2q^5 + q^4 + q^3 - q^2}{2}$.

In the second case, the equation of $T$ will be:

$$(z^2 D_0 + z D_1 + t^2)(z^2 \sigma(D_0) + z\sigma(D_1) + \sigma(t)^2),$$

which, by $\sigma(D-1)t^2 + D_1\sigma(t)^2 = C_1\alpha = C_1 t\sigma(t)$, implies $t | D_1$, so we have $q^2$ choices for $D_1$ and $q^2 - 1$ for $D_0$ for a total of $q^4 - q^2$.

It remains to count the intersection between the two cases, which happens when $f$ factors into 4 linear factors over $\mathbb{F}_{q^4}$ but not on $\mathbb{F}_{q^2}$. So the linear factor would be $(D_0 z + t)$ or $(D_0 z + \sigma(t))$, so we have $(q^4 - q^2)/4$ choices for $D_0$, times the 2 possible

terms in $x$ and $y$.

Starting from a total of $q^8 - q^7$ quartics we obtain $q^8 - q^7 - q^6 + q^5 - q^2 + 1$ irreducible quartics.

Adding together all the 3 cases we have $q^8 - q^6$ quartics which, times the choice of line and singular points, gives us $\frac{q^{12}-q^{10}-q^9+q^7}{2}$ irreducible quartics with two conjugate singular points. □

### 5.4.4 One or two singular points defined over $\mathbb{F}_q$

As anticipated at the beginning of this section, computing the number of quartics with one or two singular points defined over $\mathbb{F}_q$ is more complicated that in the previous cases. Indeed, if we approached the counting using similar methods to the one in the proofs above, we would have to consider several subcases to study the possible factorisations of $f$. For instance, we should consider all the possible different configurations of tangents lines at the singular points and all the possible intersection. This would lead to a much more complex application of the sieve principle. Therefore, we proceed in another way. The idea is to compute these cases by a brute-force code, which loops through the plane quartics defined over $\mathbb{F}_q$ for small $q$'s, in order to have enough information to interpolate the values obtained and express the counts by polynomials. Before trying this method we tried to realise the ideal of the reduced quartics with either one or two fixed $\mathbb{F}_q$-rational singular points. Is possible to define it, by writing down the generic equation of a product of two quadratics or of a product of a cubic and line, and then working out the size of the union. The problem with this method is related to the fact that to conclude we need to compute a Gröbner basis with an elimination order in a space with 27 variables: this operation is extremely expensive and slow, that would never finish in a reasonable time.

The approach we took consists in counting the number of irreducible quartics with at least two fixed singular points over $\mathbb{F}_q$ and then, subtracting the number of irreducible quartics with three (of which two are fixed) $\mathbb{F}_q$-singularities, we get the number of irreducible quartics with exactly two $\mathbb{F}_q$-singularities. Similarly, we deduct from the count of irreducible quartics with at least one singular point over $\mathbb{F}_q$ the number of irreducible quartics with exactly one $\mathbb{F}_q$-singularity (including the ones which have two conjugate singular points as well). To count how many irreducible quartics have at least two [one] fixed double points over $\mathbb{F}_q$ we can subtract from the total number of quartics with at least two [one] fixed double points over $\mathbb{F}_q$ the reducible ones. There are several reasons for doing this: the reducible ones are fewer than the irreducible ones,

indeed their cardinality is described by a polynomial of lower degree and therefore we need fewer values to interpolate; moreover it is computationally faster building reducible quartics than checking among the set of all quartics which ones are irreducible. The total number of quartics having two [one] singular points is $(q^9-1)/(q-1)$ $[(q^{12}-1)/(q-1)]$, since imposing the singularity in two [one] points is equivalent to imposing 6 [3] linear condition on the 15 coefficient of the quartics.

What is left is counting the number of reducible plane quartics having at least two [one] fixed singular points. As usual, we work with the associated polynomials to the quartics. To complete this step we wrote a script in Sage that computes all the possible reducible cases and checks whenever they are singular in the two [one] fixed point. At this stage we needed some optimisation in the code in order to smooth the computation over $\mathbb{F}_q$ when $q$ gets bigger. Indeed, we needed to reach $q = 23$ to have enough values to interpolate and therefore we need a quite efficient routine that counts the quartics. The key adjustment and improvements we implemented in the method in order to obtain an output in a reasonable time were these:

- store the quartics as just vectors of coefficients of the polynomials;
- use only scaled vectors, i.e. with the first non-zero coefficient from the right equal to 1;
- make all the computation at the level of vectors, never involving complex structures such as the polynomial ring over $\mathbb{F}_q$ or the projective plane;
- avoid double counting for the quartics, in this way we did not need to store them but just count them on the fly;
- store as little information as possible and compress the data as necessary;
- when we needed to store some items, which were essentially just reducible conics and reducible cubics, we reorganised the code in such a way we did not need to pick elements from memory but just check whenever they belonged to certain sets. This probably was the most significant improvement in terms of efficiency and speed of the code.
- Since it has a negligible cost in terms of time we counted the reducible cases with 3 fixed singular points as well. In this way we double-checked the output of the code with the value $4q^4 - 2q^3 + 3q^2 - q + 2$, known from the Proposition 5.4.1.

- Shorten the computation by working out just the coefficients we would need to evaluate if the quartics have a singularity in the fixed point. We also cut out some sub-cases and work out closed formulas for others.

- To reach the results for the biggest fields ($q = 13, 17, 19$ and $23$) we parallelized the computation. At this stage we needed to take particular care in storing as little data as possible.

Right at the start, the first version of the algorithm, had a computational time of 12 minutes single core for $q = 2$ and, since the complexity is exponential, reaching $q = 23$ was totally out of reach. After all the improvements described above we can obtain the same output in few milliseconds. The computation for $q = 23$, after solving some memory issues compressing the necessary information, was completed in 9 days running over 20-cores in parallel. The final complexity of the code is roughly $O(q^8)$ and the memory usage $O(q^7)$. Here is a table of the results.

| $q$ | One Singularity | Two Sing. | Three Sing. |
|---|---|---|---|
| 2 | 1791 | 383 | 60 |
| 3 | 49936 | 4981 | 296 |
| 4 | 554325 | 32085 | 942 |
| 5 | 3660156 | 138281 | 2322 |
| 7 | 64961856 | 1280133 | 9060 |
| 11 | 3252763152 | 26428469 | 56256 |
| 13 | 13988494716 | 81715401 | 110346 |
| 17 | 147288954636 | 505557833 | 325110 |
| 19 | 392365261200 | 1079716725 | 508632 |
| 23 | 2121064946496 | 3990825221 | 1096596 |

Interpolating these values we obtain following the two polynomials we were looking for. Having 10 values to interpolate gives us enough information to determine these polynomials. Indeed, the total number of reducible curves over $\mathbb{F}_q$ is a polynomial of degree 11; here we are fixing the coordinates of one or two singular points, since there are $q^2 + q + 1$ points in the projective plane, the degrees of the two polynomials are 9 and 7.

The number of reducible plane quartics with at least one fixed singular point:

$$q^9 + 4q^8 + 2q^7 - q^6 + q^5 + q^4 + q^3 + q^2 + q + 1.$$

The number of reducible plane quartics with at least two fixed singular points:

$$q^7 + 4q^6 - q^5 + q^4 + q^3 + q^2 + q + 1.$$

Moreover, interpolating the third column we obtain the polynomial from Proposition 5.4.1. Therefore, by taking the difference with the total number of quartics with two [one] fixed singular points, we work out the polynomial for the number of irreducible plane quartics with at least one fixed singular point:

$$q^{11} + q^{10} - 3q^8 - q^7 + 2q^6,$$

and the number of irreducible plane quartics with at least two fixed singular points is

$$q^8 - 3q^6 + 2q^5.$$

We can then work out the number of irreducible quartics with exactly one or two singularities over $\mathbb{F}_q$. Let $X_i$ the number of irreducible quartics having exactly $i$ $\mathbb{F}_q$-singularties, with $i = 1, 2, 3$. We have already an expression for $X_3$ from Proposition 5.4.1. Then, we have:

$$\begin{aligned} X_2 &= \left(q^8 - 3q^6 + 2q^5 - \frac{6X_3}{t_1(t_1-1)}\right)\binom{t_1}{2} \\ &= \frac{q^{12} + q^{11} - 2q^9 - q^8 + q^3}{2}, \end{aligned}$$

$$\begin{aligned} X_1 &= \left(q^{11} + q^{10} - 3q^8 - q^7 + 2q^6 - \frac{2X_2 + 3X_3}{t_1}\right) t_1 \\ &= \frac{2q^{13} + 2q^{12} + q^{11} - 3q^{10} - 3q^9 - q^8 + q^7 + 2q^6 - q^3}{2}. \end{aligned}$$

### 5.4.5 Smooth quartics

Having counted all the singular cases allows us to obtain the number of smooth irreducible quartics. To conclude we need to add $X_1 + X_2 + X_3$ to the count from Proposition 5.4 of irreducible ones having 3 conjugate singular points over $\mathbb{F}_{q^3}$, plus the ones from Proposition 5.5 with two conjugate singularities over $\mathbb{F}_{q^2}$ minus the only intersection between these cases, which are the ones from Proposition 5.3 with two conjugate

singularities over $\mathbb{F}_{q^2}$ and one over $\mathbb{F}_q$. Therefore, we obtain

$$q^{13} + 2q^{12} + q^{11} - 2q^{10} - 3q^9 - 2q^8 + q^7 + 2q^6 + q^5 - q^3$$

irreducible singular plane quartics defined over $\mathbb{F}_q$. Finally, we just need to subtract this polynomial from the count (5.1) of all irreducible quartics to obtain

$$q^{14} - q^{12} - q^{11} + q^9 + q^8 - q^6 - q^5 + q^3 = (q^6 + 1)|\mathrm{PGL}_3(\mathbb{F}_q)|$$

irreducible smooth plane quartics defined over $\mathbb{F}_q$.

### Smooth quartics, theoretical count

The number of smooth quartics in $\mathbb{P}^2(\mathbb{F}_q)$, which has a factor $|\mathrm{PGL}_3(\mathbb{F}_q)|$, may suggest there is a more theoretical way to count them. The following argument is due to J. Cremona and it is independent from the method above.

**Proposition 5.4.6.** *The number of smooth plane quartics in* $\mathbb{P}^2(\mathbb{F}_q)$ *is*

$$(q^6 + 1)|PGL_3(\mathbb{F}_q)|.$$

*Proof.* Let us fix a non-hyperelliptic smooth curve $C$ of genus 3 over $\mathbb{F}_q$. We embed $C$ in $\mathbb{P}^2(\mathbb{F}_q)$ through the canonical divisor $K_c$ as a degree 4 curve $\mathcal{C}$. These canonical embeddings are determined up to a change of coordinates of the Riemann–Roch space $\mathcal{L}(K_C)$ of the canonical divisor as described in Hartshorne's book [Har77, §II.5].

Since the dimension $l(K_C)$ of this space is equal to the genus of $C$ (see [Sil08, §II.5]), we have in total $G = |\mathrm{PGL}_3(\mathbb{F}_q)|$ embeddings of $C$ in $\mathbb{P}^2(\mathbb{F}_q)$. So if we count the number of different curves $\mathcal{C}$ which are embeddings of a fixed $C$, we will have $G/\#\mathrm{Aut}_{\mathbb{F}_q}(C)$, indeed if the same curve $\mathcal{C}$ is reached through two different embeddings from $C$ we can compose one with the inverse of the other to obtain an automorphism of $C$.

Then, if we sum over all the class of isomorphism of $\mathcal{C}$ over $\overline{\mathbb{F}}_q$ we get $G$ curves, by Lemma 10.7.5 of [KS99]. Once we have that is enough count the class of isomorphism over $\overline{\mathbb{F}}_q$ of quartic plane curves, which is $q^6 + 1$ by [LRRJ18, 5.3]. □

*Acknowledgement*: the author is aware that there are other references where it is possible to find similar results to the one obtained in this chapter. The techniques described in [Ber08] by Bergström are different from the ones used in this thesis and do not contain all the explicit polynomials given here. The author, during the period of his

PhD spent working on the results contained in this chapter, was not aware of Bergström's results.

# Chapter 6

# The correlation between probabilities of liftability of singular points

The aim of this chapter is to show that, given a reduction of a curve from $\mathbb{P}^2(\mathbb{Q}_p)$ to $\mathbb{P}^2(\mathbb{F}_p)$ the probabilities of lifting each of the singular points may be dependent. This fact makes the computations of chapters 8 and 9 quite complicated. Here we focus on the case of quadrics as an example, since it is the smallest degree where we have non-reduced reductions.

## 6.1 Reductions of plane quadrics

Let $Q$ be a homogeneous ternary quadric equation defined over $\mathbb{Q}$. If the set of solutions $Q(\mathbb{Q}_p)$ over the $p$-adic field is not empty then we say the quadric is solvable at the prime $p$. Moreover, any point in the set $Q(\mathbb{Q}_p)$, after rescaling $Q$ to be defined over $\mathbb{Z}$, can be reduced to a point in the set $\overline{Q}(\mathbb{F}_p)$. In general $Q(\mathbb{Q}_p)$ is not finite, for instance a double line is in bijection with $\mathbb{P}^1(\mathbb{Q}_p)$, but the set of reductions is finite, since it is a subset of the projective plane $\mathbb{P}^2(\mathbb{F}_p)$, which contains $p^2+p+1$ points. Therefore, it is natural to investigate how many points there are on the reduced curve. We can also ask the question the other way around: How many points of the reduction do lift to a point over $\mathbb{Q}_p$? We can look at the possible reductions mod $p$ and understand how many points they contain. Up to rescaling we can avoid the null quadric so the possible configurations are (here we are referring to points in $\overline{Q}(\mathbb{F}_p)$):

- a smooth conic, which contains $p+1$ smooth points;
- a double line, which contains $p+1$ singular points;
- two distinct lines, which contain $2p$ smooth points and a singular one;
- two conjugate lines, which have just one singular point.

If we have a smooth point in $\overline{Q}(\mathbb{F}_p)$, by Hensel's Lemma, it lifts to a point over $\mathbb{Q}_p$, but for the singular points we need to investigate further. Therefore, considering the possible reductions, the cardinality of image of the reduction map $Q(\mathbb{Q}_p) \to \overline{Q}(\mathbb{F}_p)$ could be either any number between 0 and $p+1$ or $2p$ or $2p+1$. Here we describe all the possible cardinalities and the probability of occurring of each case:

**Theorem 6.1.1.** *When $p$ is an odd prime and $Q$ a quadric over $\mathbb{Q}_p$ the possible cardinalities of the image $Q(\mathbb{Q}_p)$ in $\mathbb{P}^2(\mathbb{F}_p)$ through the reduction map $\pi$, with related probabilities are:*

| $n$ | $\mathbb{P}(\#\pi(Q(\mathbb{Q}_p)) = n)$ |
|---|---|
| *0* | $\frac{p}{2p^2+4p+2}$ |
| *1* | $\frac{p^6-p^5+2p^4+p^2-p+1}{2p^8+2p^7+2p^6+4p^5+4p^4+4p^3+2p^2+2p+2}$ |
| *2* | $\frac{p^4}{2p^7+2p^5+2p^4+2p^3+2p^2+2}$ |
| $\frac{p+1}{2}$ | $\frac{p^2-p}{2p^8+2p^7+2p^6+4p^5+4p^4+4p^3+2p^2+2p+2}$ |
| $\frac{p+3}{2}$ | $\frac{p}{2p^7+2p^5+2p^4+2p^3+2p^2+2}$ |
| $p$ | $\frac{p-1}{2p^8+2p^6+2p^5+2p^4+2p^3+2p}$ |
| $p+1$ | $\frac{2p^8-2p^7+2p^6-2p^5+2p^4-2p^3+1}{2p^8+2p^6+2p^5+2p^4+2p^3+2p}$ |
| $2p$ | $\frac{p-1}{2(p^2-p+1)}$ |
| $2p+1$ | $\frac{1}{2(p^2-p+1)}$ |

*When $p=2$, we have:*

| $n$ | $\mathbb{P}(\#\pi(Q(\mathbb{Q}_p)) = n)$ |
|---|---|
| *0* | $\frac{1}{9}$ |
| *1* | $\frac{67}{1134}$ |
| *2* | $\frac{37}{756}$ |
| *3* | $\frac{145}{324}$ |
| *4* | $\frac{1}{6}$ |
| *5* | $\frac{1}{6}$ |

In order to compute the probabilities described in the Theorem 6.1.1 we compute how often each reduction happens. Moreover, we refer to $t$ as the probability that a specific configuration occurs adding the condition that the quadric does not pass through the point $[1:0:0]$.

**Lemma 6.1.2.** *Among the $p^5+p^4+p^3+p^2+p+1$ ternary quadrics, up to scaling, over $\mathbb{F}_p$ we have:*

- *$p^5-p^2$ smooth conics, $t=\frac{p-1}{p}$;*
- *$p^2+p+1$ double lines, which contains $p+1$ singular points, $t=\frac{1}{p^3}$;*
- *$(p^2+p+1)(p^2+p)/2$ products of two distinct lines defined over $\mathbb{F}_p$, $t=\frac{p^2-1}{2p^3}$;*
- *$(p^4-p)/2$ products of two conjugate lines over $\mathbb{F}_{p^2}$,$t=\frac{p^2-1}{2p^3}$.*

Those quantities are described in the second section of [BCF15a]. Part of the probabilities above are from [BCF+15b], the remaining ones come from an easy computation.

## 6.2 Probabilities of the number of liftable points

Now we need to understand how many points lift for each configuration. As described above all the smooth points would lift, so we need to compute the probabilities of lifting for each specific singular point.

It follows that for the smooth conics we always have $p+1$ points lifting.

In case of a product of two conjugate lines we can have either 0 or 1 point, depending on the liftability of the $\mathbb{F}_p$-rational singular intersection. This probability can be read also as the probability that the curve is solvable over $\mathbb{Q}_p$, since at most one point can lift. So, by the results in Section 3.4 of [BCF+15b] we have that the solubility of this case is $\alpha_1^{(3)} = \frac{1}{p+1}$, using the notation of that paper. Therefore, when the reduction is a product of conjugate lines we have no points lifting with probability $\frac{p}{p+1}$, and one point lifting with probability $\frac{1}{p+1}$.

If the reduction is a product of two distinct lines we have $2p$ smooth points that lift, plus the undetermined singular one, which we now consider. We can move the two lines to $x = 0$ and $y = 0$, so the equation $f$ of the reduced quadric $\overline{Q}$ is $xy = 0$. Now, since we want to lift the intersection point $[0 : 0 : 1]$, we substitute $x \to px$ and $y \to py$ and then reduce the equation by $p$ we get $az^2 = 0$; by primitivity, $z \neq 0$, so we need $v_p(a) > 0$, which happens with probability $1/p$. Therefore, we can divide again by $p$ and get the equation $\gamma : xy + z(bx + cy) + a'z^2 = 0$. This conic $\gamma$ intersects the line $z = 0$ in two distinct $\mathbb{F}_p$ points, therefore the conic is either a product of two $\mathbb{F}_p$-lines or a smooth conic; in both cases, in the open affine $Z \neq 0$ there are smooth points, so the intersection point does lift. In conclusion when the reduction is a product of two $\mathbb{F}_p$-lines, $2p$ points lift with probability $\frac{p-1}{p}$ and $2p + 1$ points lift with probability $\frac{1}{p}$.

The remaining case, the double line, needs some dedicated computation. Indeed, even though its solubility was described in [BCF+15b], this information there can be used to determine just the probability that no points lift; but the probabilities of any possible cardinality are analysed in the following:

**Lemma 6.2.1.** *If the reduction $\overline{Q}$ is a line squared, then the possible number of points lifting and their probabilities when $p \geq 3$ are*

| $n$ | $\mathbb{P}(\#\pi(Q(\mathbb{Q}_p)) = n)$ |
|---|---|
| *0* | $\frac{p}{2p+2}$ |
| *1* | $\frac{p^4+p^3+1}{2(p^5+p^4+p^3+p^2+p+1)}$ |
| *2* | $\frac{p^4}{2(p^4+p^2+1)}$ |
| $\frac{p+1}{2}$ | $\frac{p(p-1)}{2(p^5+p^4+p^3+p^2+p+1)}$ |
| $\frac{p+3}{2}$ | $\frac{p}{2(p^4+p^2+1)}$ |
| $p$ | $\frac{p-1}{2(p^5+p^3+p)}$ |
| $p+1$ | $\frac{1}{2(p^5+p^3+p)}$ |

*When $p = 2$, we have:*

| $n$ | $\mathbb{P}(\#\pi(Q(\mathbb{Q}_p)) = n)$ |
|---|---|
| *0* | $\frac{1}{3}$ |
| *1* | $\frac{25}{126}$ |
| *2* | $\frac{37}{84}$ |
| *3* | $\frac{1}{36}$ |

*Proof.* We move the double line to $x = 0$, then the reduction is $x^2 = 0$. The triangle describing the valuations of the coefficients of the conics $Q$ over $\mathbb{Q}_p$ is as follows

$$\begin{array}{cccccc} Z^2 & \geq 1 & & & \\ & \geq 1 & \geq 1 & & \\ X^2 & = 0 & \geq 1 & \geq 1 & Y^2 \end{array}$$

After substituting $x$ with $px$ and dividing by $p$, the reduction is a binary quadric, which among all the possible $p^3$ quadrics can have different roots over $\mathbb{F}_p$:

- two distinct roots over $\mathbb{F}_p$, in $p(p^2-1)/2$ cases, here two points lift;

- two conjugate roots over $\mathbb{F}_{p^2}$, in $(p-1)^2p/2$ cases, which implies no solubility by primitivity;
- a double root over $\mathbb{F}_p$, in $p^2-1$ cases, which implies that at most one point would lift;
- a null quartic, just in one case, which leaves us with no information about the $p+1$ singular points.

We continue the investigation in the last two cases. When we have a double root we move it to $y=0$, so the reduction is $y^2=0$, by the substitution $y \to py$ and dividing by $p$ we have

$$\begin{array}{llll} Z^2 & \geq 0 & & \\ & \geq 0 & \geq 1 & \\ X^2 & = 0 & \geq 1 & = 1 \quad Y^2 \end{array}$$

which describes a monic binary quadric. With probability $(p-1)/(2p^2)$ we have two distinct roots, so we got one point lifting. If the two roots are conjugate by primitivity we have no lifting and if there is a double root (with probability $1/p$) we iterate the process (moving the root to $x=0$, substituting $x \to px$ and dividing by $p$) ending in the same reduction with $x$ and $y$ swapped. Therefore, the solubility $\tau$ in this case would be the same, and we can write a recursive formula:

$$\tau = \frac{p-1}{2p^2} + \frac{1}{p}\tau,$$

hence $\tau = \frac{1}{2}$.

Instead, if the reduction is null, we can still lift any of the $p+1$ points. Dividing by $p$ we get the following:

$$\begin{array}{llll} Z^2 & \geq 0 & & \\ & \geq 0 & \geq 0 & \\ X^2 & = 0 & \geq 0 & \geq 0 \quad Y^2 \end{array}$$

which is a generic quadric not passing through the point $[1:0:0]$. Now, the set of the singular points coming from $x^2=0$, can be represented by the set $S$ of all the lines through the point $[1:0:0]$; if one of those lines, with equation $\lambda y + \mu z = 0$, does intersect the quadric in a smooth point then the associated point $[0:\mu:\lambda]$ on $x=0$ lifts.

If the reduction is the product of two conjugate lines we can have just one possible point to lift and, as described above, this happens with probability $\alpha_1^{(3)} = \frac{1}{p+1}$, otherwise we have no points lifting.

If the reduction is the product of two distinct lines when we intersect it with lines in $S$ we get in $p$ cases smooth points and in one case just a singular one (when we are considering the line passing through the singular point of the quadric). Then we have at least $p$ points lifting, moving the remaining singular one to $[0:0:1]$ we can determine if it does lift or not. The equation of the reduction is now $x(x+y) = 0$, substituting $x \to px$ and $y \to py$ and dividing by $p$ the reduction is $\overline{a_{0,0,2}}z^2 = 0$. By primitivity $z \neq 0$, we can lift this point if and only if $\overline{a_{0,0,2}} = 0$, which happens with probability $1/p$. Therefore, dividing again by $p$ the reduction becomes

$$\begin{array}{llll} Z^2 & \geq 0 & & \\ & \geq 0 & \geq 0 & \\ X^2 & = 0 & = 0 & \geq 1 \quad Y^2 \end{array}$$

This quadric has two $\mathbb{F}_p$ points on the line $z = 0$, therefore is either a smooth conic or a product of two lines over $\mathbb{F}_p$. In both cases this implies that there exists one smooth point with $z$-coordinate not null on the reduction, so we can apply Hensel's Lemma. Summarising, we have $p$ points lifting in this case with probability $\frac{p-1}{p}$, and $p+1$ with probability $\frac{1}{p}$.

In the case the reduction is a smooth conic we have to consider small $p$ separately. If $p = 2$, the three lines in $S$ can be either all tangents to the conic with intersection defined over $\mathbb{F}_p$ with probability $3/4$, giving 3 points lifting (the maximum possible, since $p+1 = 3$), or there can be one tangent, one secant with intersections defined over $\mathbb{F}_p$ and another with two conjugate intersections over $\mathbb{F}_{p^2}$, giving 2 points lifting, with probability $1/4$.

If $p \geq 3$, we can either have: $(p+1)/2$ lines in $S$ which are secant in $\mathbb{F}_p$ points, giving so $(p+1)/2$ points lifting with probability $(p-1)^2/2p^2$ or two tangents and $(p-1)/2$ secants in $\mathbb{F}_p$, giving $(p+3)/2$ points lifting with probability $(p^2-1)/2p^2$.

It remains to consider the double line, which happens with probability $1/p^3$, considering the condition of having a null binary quadric, this happens with probability $1/p^6$ starting from the initial setting. We end up in the same initial configuration, and hence each configuration can happen again, weighted with a probability $1/p^6$, and reaching the double conic we would iterate again. In conclusion, we can compute the final probability of each cardinality of points lifting by multiplying the one computed after one iteration times all the weights, which are:

$$\sum_{k=0}^{\infty}\left(\frac{1}{p^6}\right)^k = \frac{p^6}{p^6-1}.$$

Adding all the probabilities cited above we compute the probabilities as given in the tables of the statement. □

In order to compute the results described in Theorem 6.1.1, we add all the probabilities for any fixed cardinality and weight them by the probability of being in the respective reduction.

*Remark* 6.2.2. The distribution of the number of points lifting gives us some insight about their nature. Indeed, the number of the possible cardinalities is just 9, clustered around 4 values: almost none (0,1,2), roughly half $p$ ($\frac{p+1}{2}$, $\frac{p+3}{2}$), roughly $p$ ($p$, $p+1$) and roughly twice $p$ ($2p$ and $2p+1$) but a priori they could be any possible values between 0 and $2p+1$. The most interesting case is when the reduction is a line squared, indeed we have $p+1$ points which may look equally "liftable" but their probabilities of lifting are not at all independent. This detail causes trouble when we try to evaluate the probability in a more complicated setting, such as the quartics which have non-reduced reductions (e.g. when the quartic mod $p$ is a power of a lower degree curve).

# Chapter 7

# Probabilities of solubility for undetermined cases

This chapter is dedicated to the computation of the probabilities of solubility of the undetermined cases that have been described in the last chapter. Once we have completed this task, we will be able to weight those probabilities with the density of the respective reductions mod $p$, and hence we will be able to compute the overall probability of solubility for a quartic in $\mathbb{Q}_p$. There will be some restriction on $p$, for instance we will assume it to be greater than 29; this condition is due to the Hasse-Weil bound, as for smaller $p$ there are smooth quartics which do not have a point, see [HLT05]. In order to study the solubility of each configuration we apply some techniques similar to those used in [BCF15a] to compute the probability of solubility of the ternary cubics, while in some cases we introduce some new methods to understand the probabilities involved. It is possible to picture the entire procedure as an algorithm that detects if a specific quartic has a point or not over $\mathbb{Q}_p$ by looking at sequential reduction mod $p$ of the quartic itself. In practice, we gather information on the original curve, increasing step by step the precision of its coefficients until we are able to conclude if it contains a point or not. In certain situations this procedure may not end but enters in a "loop", at which stage we can describe the solubility by a recursive formula. This method, if implemented on an explicit quartic instead of an family, basically detects if a quartic is soluble or not; it is guaranteed to terminate since at each step the discriminant of the quartic studied decreases. Details about this kind of algorithms have been studied and implemented by N. Bruin in section 5 of [Bru06]. Another possibility is that the configuration reached through the algorithm can be related to other configurations, and therefore we link their probabilities of solubility by linear equations. Once the list of

linear equations is complete, we are able to solve the linear system and work out the solubility of each reduction type.

For brevity, in what follows we will say that a subset of quartics "has solubility $\rho$" to mean that the conditional probability of solubility, given that a quartic lies in the subset, is $\rho$.

## 7.1 Standard techniques

As described above we are going to study the solubility of the undetermined cases by looking at the reduction mod $p$ of the quartics. All the undetermined cases are reductions which have $\mathbb{F}_p$ points (otherwise they would be bad cases with solubility 0) but all of them are singular (otherwise we would have a good case with solubility 1). We can act on these reductions, which are curves in $\mathbb{P}^2(\mathbb{F}_p)$, by a linear change of coordinates, this would not affect the probability of solubility of the quartics over $\mathbb{Q}_p$. Indeed, a change of coordinates over $\mathbb{P}^2(\mathbb{F}_p)$ can be described by an element of $\mathrm{PGL}_3(\mathbb{F}_p)$; then, since the map $\mathrm{PGL}_3(\mathbb{Z}_p) \to \mathrm{PGL}_3(\mathbb{F}_p)$ is surjective, we lift it to an element of $\mathrm{PGL}_3(\mathbb{Z}_p)$ which acts on the quartics defined over $\mathbb{Q}_p$, those changes of variables preserve the Haar measure, so the probability of solubility is invariant with respect to the action of these elements. Therefore, we can move up to 4 points in general position to any other 4 points in general position of the projective plane. This procedure allows us to deal with simplified equations which have sparse coefficients.

For example, suppose we are interested in whether the quartic $T = 0$ contains a point $[x : y : z]$ which reduces to some fixed point $[\overline{x} : \overline{y} : \overline{z}] \in \mathbb{P}^2(\mathbb{F}_p)$. By a linear change of variables we may assume that $[\overline{x} : \overline{y} : \overline{z}] = [1 : 0 : 0]$, and hence $p|y$ and $p|z$. Writing $y = py'$ and $z = pz'$ leads us to consider solubility of the new quartic $T' = T(X, pY, pZ) = 0$, with the constraint that now we are only interested in points $[x : y' : z']$ on $T' = 0$ for which $p \nmid x$.

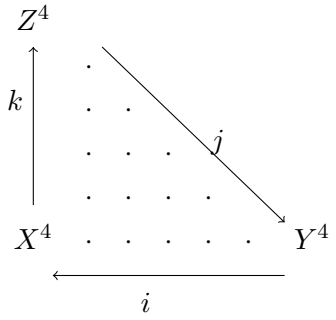
If, after such a scaling of coordinates, we obtain a quartic where all of whose coefficients are divisible by $p$, we will always divide by $p$ before continuing, so that at each stage we may assume that the reduction of $T$ modulo $p$ is not identically zero.

There are three conditions that allow us to end the procedure:

- The reduction contains a smooth $\mathbb{F}_p$-rational point, therefore we have solubility.
- The reduction contains no $\mathbb{F}_p$-rational point apart from points which contradict the original primitivity assumption, therefore we have insolubility.

- The reduction coincides with a known one, therefore we can link the solubilities of the two cases by linear equations.

In most cases, all three outcomes are possible for the same initial reduction type, depending on the coefficients of the quartics. At each stage we split the computation in subcases, imposing congruence conditions on the coefficients. We use the notation $c(X^iY^jZ^k)$ for the coefficient of the monomial $X^iY^jZ^k$. Since most of the computations involve the valuations of the coefficients of the quartics $T$ over $\mathbb{Z}_p$ we represent them in a triangle, where for each point the distance from each vertex determines the exponent of each variable and the value is the valuations of the coefficient of the associated monomial.




where each dot refers to $v(c(X^iY^jZ^k))$, i.e. the valuation of the coefficient of the monomial $X^iY^jZ^k$, for one of the 15 triples $(i,j,k)$. For instance if the reduction $\overline{T}$ is a quadruple line which, after a suitable change of coordinates, we may assume is $X^4 = 0$. In this case, from the reduction we have information only on the coefficient of $X^4$, which has valuation 0, while all the other coefficients have valuation $\geq 1$, therefore the triangle of valuations would look like this:

$$\begin{array}{lllllll} Z^4 & \geq 1 & & & & & \\ & \geq 1 & \geq 1 & & & & \\ & \geq 1 & \geq 1 & \geq 1 & & & \\ & \geq 1 & \geq 1 & \geq 1 & \geq 1 & & \\ X^4 & = 0 & \geq 1 & \geq 1 & \geq 1 & \geq 1 & Y^4 \end{array}$$

## 7.2 Probability tools and further counts

Throughout the detailed computation of the probabilities of each case, we will need some general results; we list most of them here in order to make the exposition clearer.

Sometimes the reduction of the quartic over $\mathbb{F}_p$ is a double line times a quadratic whose coefficients are parametrized by polynomials in one variable; for instance this happens in the proof of Proposition 7.3.13. The solubility of those configurations is related to the factorisation of the quadratic, which is described for odd $p$ by the Legendre symbol of its discriminant.

We consider a parametrized quadratic $M(b,X) = h(b)X^2 + g(b)X + 1$, where $h, g \in \mathbb{F}_p[b]$. For each $b \in \mathbb{F}_p$, $M(b,X)$ has either distinct roots in $\mathbb{F}_p$, a double one in $\mathbb{F}_p$ or two conjugate ones in $\mathbb{F}_{p^2}$, according to the value of the Legendre symbol $\left(\frac{\Delta(b)}{p}\right)$ where $\Delta(b) = g^2 - 4h$.

Therefore, defining the set $S$ as $S := \left\{ \left(\frac{\Delta(b)}{p}\right) : b \in \mathbb{F}_p \right\}$, we say that $M$ is

(i) *Good*, if $1 \in S$, i.e. there exists a $\overline{b}$ such that the polynomial $M(\overline{b}, X)$ has two distinct roots on $\mathbb{F}_p$.

(ii) *Bad*, if $S = \{-1\}$, i.e. for any $b \in \mathbb{F}_p$ $M(b,x)$ has two conjugate roots on $\mathbb{F}_{p^2}$.

(iii) *Undetermined*, if $\{0\} \subseteq S \subseteq \{0,-1\}$, i.e. there are no $b$ such that the polynomial $M(\overline{b}, X)$ has two distinct roots on $\mathbb{F}_p$ but there exists one for which $M$ has a double root.

**Lemma 7.2.1.** *Let $p > 17$ be a prime and $h(b)$ and $g(b)$ be two polynomials in $\mathbb{F}_p[b]$, whose degrees are bounded respectively by 4 and 3.*

*Let $u$ be the leading coefficient of $\Delta(b)$, the discriminant of $M(b,X) = h(b)X^2 + g(b)X + 1$, where $M$ is the polynomial described above. Then, we have the following count for all the possible cases for $T$:*

| $\deg(\Delta)$ | $\left(\frac{u}{p}\right)$ | Good | Undetermined | Bad |
|---|---|---|---|---|
| 0[1] | $\pm 1$ | $\frac{p-1}{2}$ | 1 | $\frac{p-1}{2}$ |
| 1 | $\pm 1$ | $p^2 - p$ | 0 | 0 |
| 2 | 1 | $\frac{p-1}{2}p^2$ | 0 | 0 |
| 2 | $\pm 1$ | $\frac{2p^3-3p^2+p}{2}$ | $\frac{p^2-p}{2}$ | 0 |
| 3 | $\pm 1$ | $(p-1)p^3$ | 0 | 0 |
| 4 | 1 | $\frac{p-1}{2}p^4$ | 0 | 0 |
| 4 | $\pm 1$ | $\frac{2p^5-2p^4-p^3+p^2}{2}$ | $\frac{(p-1)(p^2+p)}{4}$ | $\frac{(p-1)(p^2-p)}{4}$ |
| 6 | 1 | $\frac{p-1}{2}p^6$ | 0 | 0 |

[1]We are including in the case of $deg(\Delta) = 0$ the null polynomial $\Delta = 0$, which is undetermined.

*Proof.* First of all, we refer to an argument of M.Bhargava, J. Cremona, and T. Fisher from [BCF]. They proved that when $p \geq \deg \Delta^2$ if $\Delta(b)$ is not of the form $u't^2(b)$, with $u'$ non-quadratic residue and $t \in \mathbb{F}_p[b]$, then $M$ is good. Their proof, adapted to our setting, is the following. According as $\deg(\Delta)$ is odd or even we write $\deg(\Delta) = 2i+1$ or $2i+2$. We write $\Delta = \Delta_1 t^2$ where $\Delta_1$ and $t \in \mathbb{F}_p[b]$, with $\Delta_1$ squarefree. If $\deg(\Delta_1) \geq 1$, then the Hasse-Weil bound gives a lower bound of $(p - 1 - 2i\sqrt{p})/2$ for the number of elements $\bar{b}$ in $\mathbb{F}_p$ such that $\Delta_1(\bar{b})$ is a square. Since the number of roots of $t$ is at most $i$, if $p > (2i+1)^2$, the polynomial $M$ is good. If $\Delta_1 = c$ is a constant, then in the case $\left(\frac{c}{p}\right) = +1$ the polynomial $M$ is good if there exists an element of $\mathbb{F}_p$ that is not a root of $t$, which exists when $p > g + 1$.

To complete the proof of this Lemma, it remains to discuss, for even degrees, when $\Delta(b) = u't^2(b)$, with $u'$ a non-quadratic residue. These cases are the undetermined and bad ones.

If $\Delta(b)$ is the null polynomial then $M$ is an undetermined case.

When the degree of $\Delta$ is zero we have $(p-1)/2$ choices for $u'$ that correspond to $(p-1)/2$ bad polynomials.

When the degree of $\Delta$ is two, $t$ is a linear polynomial, hence it has a root and therefore $M$ is undetermined. We have $p$ choices for $t$ and $(p-1)/2$ for $u'$.

When the degree of $\Delta$ is four, $t$ can be either irreducible over $\mathbb{F}_p$, in such case $M$ is bad, or having at least one root, in this case $M$ is undetermined. In the first case there are $(p^2 - p)/2$ possible $t$, in the second $(p^2 + p)/2$; times $(p-1)/2$ choices for $u'$.

To conclude, it is possible to obtain a sharper lower bound for $p$, instead of $p > \deg(\Delta)^2$. Indeed, by an exhaustive method for the polynomials defined over small prime fields, we worked out that $p > 17$ is sufficient. □

Another general result we will use during the computation of the probabilities is related to the distribution of the values of a polynomial at a fixed set of elements.

In the following Theorem we consider polynomials $f(x) \in \mathbb{F}_p[x]$ whose coefficients are random $\mathbb{F}_p$-valued variables.

**Theorem 7.2.2.** *Let $B = \{b_1, \ldots, b_k\} \subset \mathbb{F}_p$ be a set of $k$ distinct elements in $\mathbb{F}_p$. Let $f(x) \in \mathbb{F}_p[x]$ be a random polynomial whose first $k$ coefficients are uniformly distributed over $\mathbb{F}_p^k$ and are independent of the remaining coefficients. Then the values $f(b_1), \ldots, f(b_k)$ are also uniformly distributed*

*Proof.* Let $P$ be the $k \times (n+1)$ matrix $(b_i^j)$, let $F$ be the vector column of the coeffients $f_i$ of $f(x)$ and let $V$ be the vector column of the $k$ values $f(b_i)$ of the polynomial $f$ at

the elements $b_i$. Since $P$ is a Vandermonde matrix and the $b_i$ are distinct, the first $k$ columns of $P$ form an invertible matrix $E$. Let $C$ be the matrix made by the last $n+1-k$ columns of $P$, in such a way we have $P = (E|C)$. It follows that

$$V = PF = EF_0 + CF_\infty,$$

where $F_0$ is the column vector with the first $k$ entries of $F$ and $F_\infty$ is the remaining part of $F$. Now $F_0 \in \mathbb{F}_p^k$ is uniformly distributed and independent of $F_\infty$. $E$ and $C$ are constant (depending only on $B$), so $V$ is uniformly distributed as well.

□

## 7.3 Local conditions for solubility

In some cases it is not necessary to impose conditions on the whole set of coefficients of the quartics to determine the probability that they are solvable. Indeed, it is sometimes possible to investigate just the local structure of the quartic at the singular points, where the adjective local refers to geometric behaviour of the curve at one point, and not that we are considering solubility over the local field $\mathbb{Q}_p$. In detail, we want to describe the probability that a specific point would lift given just information about the tangent lines to the curve at the singular point. In the cases of semi-stable reduction, which have just ordinary double singularities, there are just two possible scenarios that may occur: two distinct tangent lines defined over $\mathbb{F}_p$ or two conjugate lines over $\mathbb{F}_{p^2}$. However, in order to describe the probability of lifting a double point in the general case, we describe here the case with a double tangent as well.

We start with the easiest case: two distinct tangents defined over $\mathbb{F}_p$.

**Proposition 7.3.1.** *Let $T$ a ternary homogeneous quartic over $\mathbb{Z}_p$. If its reduction $\overline{T}$ contains a singular point $P$ with two distinct tangent lines defined over $\mathbb{F}_p$, then the probability that $P$ lifts to a point over $\mathbb{Q}_p$ is $1/p$.*

*Proof.* Let us move the singular point $P$ to $[0:0:1]$, then the reduction of $T$ is

$$\overline{T} := z^2 L_1 L_2 + z C_3 + C_4,$$

where $L_1$ and $L_2 \in \mathbb{F}_p[x, y]$ are the tangent lines at $P$ and the $C_i$'s are forms of degree $i$ in $x$ and $y$. In order to lift $P$ we substitute $X$ with $pX$ and $Y$ with $pY$ in $T$. Dividing

the resulting quartic, which we rename $T$, by $p$ we obtain

$$\overline{T} := uz^4.$$

Since the $z$-coordinate of $P$ is not zero by primitivity, $u$ has to be zero, which corresponds to the second $p$-adic digit of $a_{0,0,4}$ (the first one is zero by the fact that $P$ is a point in the reduction). This happens with probability $1/p$. Assuming $u = 0$ we can divide again by $p$ and (with $u/p$ replaced by $u$) obtain

$$\overline{T} = z^2(uz^2 + vxz + wyz + L_1L_2) = z^2\gamma.$$

By the same argument as above, which is basically the primitivity of the coordinates of $P$, we cannot lift any point on the line $z = 0$, therefore we need to look for points just on the conic $\Gamma$ defined by $\gamma = 0$. The intersection between $\Gamma$ and the line $z = 0$ is two distinct $\mathbb{F}_p$ points, therefore $\Gamma$ can be either a smooth conic or a product of two distinct $\mathbb{F}_p$ lines. In both cases we do have a smooth point to lift, and therefore we find a lift of $P$. In conclusion we had to impose just one condition on the first digit of $a_{0,0,4}$ and therefore the liftability of $P$ occurs with probability $1/p$.

□

The next proposition is about the case with two conjugate tangents. We are interested in understanding how the liftability of a specific point depends on the liftability of other points, since our aim is to compute the probability that at least one point lifts. In the proof below we describe in detail the conditions on the coefficients of the quartic, so that later we will be able to work out the dependency of liftability between several singular points.

**Proposition 7.3.2.** *Let $T$ be a ternary homogeneous quartic over $\mathbb{Z}_p$. If its reduction $\overline{T}$ contains a double point $P$ with two conjugate tangent lines then the probability that $P$ lifts to a point over $\mathbb{Q}_p$ is $\frac{1}{p+1}$.*

*Proof.* First of all we move the point of intersection to $P = [0 : 0 : 1]$ so the reduction is

$$\overline{T} = z^2L\sigma(L) + zC_3 + C_4,$$

where $L$ and $\sigma(L)$ are the conjugate tangent lines at $P$ and $C_i$ are forms of degree $i$ in $x$ and $y$.

The first substitution we apply is $pX \to X$ and $pY \to Y$, then we divide by $p$ and we obtain $uz^4 = 0$ as reduction. Since, by primitivity, we cannot have $z = 0$ this forces

$u \equiv 0 \pmod{p}$ which happens with probability $1/p$. This give us a necessary condition on the $p$-adic coefficient of $Z^4$, i.e. $v(a_{0,0,4}) \geq 2$. Then, dividing again by $p$, the reduction we obtain is

$$\overline{T} = z^2(uz^2 + vxz + wyz + L\sigma(L)) = z^2\gamma.$$

Let us refer to the solubility of this case as $\tau$. By primitivity we cannot lift points on $z = 0$, so we can just look for points on $\gamma$ but not on $z = 0$. Notice that the intersection between $\gamma$ and $z = 0$ are two conjugate points.

Here we can make a change of coordinates that vanishes the two coefficients $v$ and $w$. Let $L\overline{L} = ax^2 + bxy + cy^2$, then make the following change of coordinates:

$$\begin{aligned} x' &= x + \frac{wb - 2cv}{4ac - b^2}z \\ y' &= y + \frac{vb - 2av}{4ac - b^2}z \\ z' &= z. \end{aligned}$$

Notice that since $L\overline{L}$ do not factor over $\mathbb{F}_p$ its discriminant $\Delta = b^2 - 4ac$ is not zero. After this change of coordinates, the reduction is

$$\overline{T} = z^2(u'z^2 + ax^2 + bxy + cy^2) = z^2\gamma',$$

with the same $a, b$ and $c$ as above and $u' = u + \phi$, where $\phi = \frac{cv^2 - bvw + aw^2}{b^2 - 4ac}$. The conic $\gamma' = 0$ is irreducible if and only if $u' \neq 0$, which is equivalent to $u = \frac{a_{0,0,4}}{p^2} \neq -\phi$. In the case the conic is irreducible we have solubility, indeed we will have a smooth point on the reduction of the quartic, then by Hensel's lemma we can lift it to a point over $\mathbb{Q}_p$. Therefore, since $u$ is uniformly distributed, this happens with probability $\frac{p-1}{p}$. In the case $\gamma$ is reducible (which happens with probability $1/p$), since the intersection with $z = 0$ are two conjugate points, it can just be the product of two conjugate lines which do not intersect on $z = 0$. The quantity $\phi$ above can be computed in a more natural way: instead of changing the coordinates we can check the irreducibility of $\gamma$ directly. Indeed, using the Laplace formula, we have that the determinant of the associated matrix of $\gamma$ can be expressed as $u$ times the minor associated to the two lines, which is non-zero, plus other terms. Since the determinant is linear in $u$ for any possible choice of the other coefficients there exists just one value of $u \in \mathbb{F}_p$ that gives a zero discriminant: this value is $-\phi$.

Then we apply the same substitution $pX \to X$ and $pY \to Y$, again divide by $p$ and obtain $cz^4 = 0$ as reduction. Again we cannot have $z = 0$ by primitivity; this

forces $u \equiv 0 \pmod{p}$ which happens with probability $1/p$. Then, dividing again by $p$, the reduction obtained is the same described above, which has solubility $\tau$. Therefore, we have a recursive formula to compute $\tau$, indeed we have

$$\tau = \frac{p-1}{p} + \frac{\tau}{p^2},$$

which implies $\tau = \frac{p}{p+1}$, Then the overall solubility in this case is

$$\frac{\tau}{p} = \frac{1}{p+1}.$$

□

*Remark* 7.3.3. Notice that throughout the preceding proof, we only imposed linear conditions which involve the coefficient $a_{0,0,4}$ of $z^4$. Indeed, in the change of variables that moves the singular point to $[0:0:1]$ when $\gamma$ is reducible, we obtain a new value for $a_{0,0,4}$ but, since the change of variables is linear, its distribution is not affected. Therefore, the solubility is independent of the values of all coefficients but $a_{0,0,4}$. In particular, we can explicitly write down the condition of solubility on the coefficient $a_{0,0,4}$. Let $\phi_n$ be the value we add to $u$ after the change of coordinate at the $n^{\text{th}}$ iteration of the procedure, this value depends on $a, b$ and $c$, which are the zero digits of three coefficients of the quartic over $\mathbb{Q}_p$, namely $\overline{a_{2,0,2}}, \overline{a_{1,1,2}}, \overline{a_{0,2,2}}$, and also on $v$ and $w$, which are the $n^{\text{th}}$ digits of $a_{1,0,3}$ and $a_{0,1,3}$. Instead $u$ is the $2n^{\text{th}}$ digit of $a_{0,0,4}$, so we can write the condition of solubility as follows:

The important point to note here is that the solubility depends only on the value of $a_{0,0,4}$.

**Corollary 7.3.4.** *A singular point with two conjugate tangent lines, after a suitable change of coordinates that sends it to* $[0:0:1]$*, lifts if and only if there exist a positive integer* $m$ *such that the* $p$*-adic expansion of* $a_{0,0,4}$ *to precision* $o(2^{2m+3})$ *is*

$$\sum_{i=1}^{m} -\phi_i p^{2i} + r p^{2m+2}$$

*where* $r \neq -\phi_{m+1}$ *and the* $\phi_m$ *are the terms described in the proof of Proposition 7.3.2 (*$\phi$ *in the proof corresponds to* $\phi_1$*, the other terms come from the iteration).*

The remaining case, which does not occur for quartics with semi-stable reduction, is when there is a single double tangent. Even though we do not need it directly to compute the solubility of the semi-stable reduction we add this case for completeness.

Moreover, in this way we can compute the probability of solubility of a singular double point. This particular case ends up to be more complicated than the previous ones. The complexity is due to a non-reduced reduction that appears in the procedure: the product of two double lines. The key problem with the product of two double lines is that the singular points are no more isolated and their cardinality is not constant but linear in $p$. The hard work here is to understand the dependency of liftability between the singular points on the double lines, indeed during the procedure we will have $p$ possible points to lift. Since the computation of this probability of solubility involves several steps we define some auxiliary solubilities, in order to have a clearer exposition and use these formulas even in other cases than just the solubility of a point with a double tangent.

**Definition 7.3.5.** *Let $k$ be a positive integer and $T(X,Y,Z)$ be a quartic over $\mathbb{Z}_p$ whose triangle of valuation is*

$$\begin{array}{cccccccc} Z^4 & \geq 2k & & & & & & \\ & \geq k & \geq 2k & & & & & \\ & \geq 1 & \geq k & \geq 2k & & & & \\ & \geq 1 & \geq 1 & \geq k & \geq 2k & & & \\ X^4 & \geq 1 & \geq 1 & = 0 & \geq k & \geq 2k & Y^4 \end{array}$$

*We define $\omega_k$ to be the probability of solubility of the quartic, given that is not possible to lift any point whose $x$-coordinate (i.e. the coordinate of the point reduced to $\mathbb{F}_p$) is zero.*

On the side of those variable we need others, which are similar, but not equal, to the previous ones.

**Definition 7.3.6.** *Let $k$ be a positive integer and $T(X,Y,Z)$ be a quartic over $\mathbb{Z}_p$ whose triangle of valuation is*

$$\begin{array}{cccccccc} Z^4 & \geq 4 & & & & & & \\ & \geq k & \geq 4 & & & & & \\ & \geq 2 & \geq 2 & \geq 4 & & & & \\ & \geq 1 & \geq 1 & \geq 2 & \geq 4 & & & \\ X^4 & \geq 1 & \geq 1 & = 0 & \geq 2 & \geq 4 & Y^4 \end{array}$$

*We define $\chi_k$ to be the probability of solubility of the quartic, given that is not possible to lift any point whose $x$-coordinate (i.e. the coordinate of the point reduced to $\mathbb{F}_p$) is zero.*

Notice that $\chi_1 = \omega_2$.

Our aim is link these solubilities $\omega_k$ and $\chi_k$ by linear equations and then be able to express them as rational functions of $p$. We will proceed as follows: first we will write

$\omega_1$ in function of $\omega_2$, $\chi_2$ and $\chi_3$, then $\omega_2$ in function of $\omega_3$ and $\chi_3$, then $\chi_2$ in function of $\chi_3$ and finally, realising that $\chi_3 = \chi_k$ for any $k$ greater or equal than 3, we will have a recursive function for $\chi_3$.

**Lemma 7.3.7.**

$$\begin{aligned}\omega_1 =& \frac{8p^9 - 2p^8 + 4p^7 - 22p^6 + 24p^5 - 6p^3 - 6}{12p^9} \\ &+ \frac{(\omega_2 + \chi_2)(12p^6 - 12p^5) + \chi_3(3p^3 + 6p^2 - 9p + 12)}{12p^9}.\end{aligned}$$

*Proof.* In order to link $\omega_1$ to $\omega_2$ we basically compute the solubility $\omega_1$. Let $T$ be a quartic satisfying the conditions for $\omega_1$ described in the Definition 7.3.5. We have that the triangle of valuations of the coefficients of $T$ described in Table 7.1.

| | | | | | |
|---|---|---|---|---|---|
| $Z^4$ | $\geq 2$ | | | | |
| | $\geq 1$ | $\geq 2$ | | | |
| | $\geq 1$ | $\geq 1$ | $\geq 2$ | | |
| | $\geq 1$ | $\geq 1$ | $\geq 1$ | $\geq 2$ | |
| $X^4$ | $\geq 1$ | $\geq 1$ | $= 0$ | $\geq 1$ | $\geq 2$ | $Y^4$ |

Table 7.1: Quartic with solubility $\omega_1$.

Then, the reduction $\overline{T}$ is the product of two lines squared we have as equation $x^2y^2 = 0$, but we cannot lift points on $x = 0$ by primitivity.

$\omega_1$ is the probability of lifting at least one double point (excluding the quadruple point $[0 : 0 : 1]$) on the line $y = 0$. We pick the point $[1 : 0 : b]$ on the line $y = 0$ and we move it to $[1 : 0 : 0]$, by the change of coordinates who fixes $x$ and $y$ and sends $z$ to $z + bx$, we therefore have that $p|Y$ and $p|Z$. Since we want the probability of lifting at least one point we keep track of this change of coordinates, in certain configurations having the freedom to vary $b$ will guarantee solubility. In particular, we are interested in the new coefficients of some specific monomials. After the change of coordinates, we have:

$$\begin{aligned}a'_{4,0,0} &= a_{4,0,0} + ba_{3,0,1} + b^2a_{2,0,2} + b^3a_{1,0,3} + b^4a_{0,0,4}, \\ a'_{3,0,1} &= a_{3,0,1} + 2ba_{2,0,2} + 3b^2a_{1,0,3} + 4b^3a_{0,0,4}, \\ a'_{3,1,0} &= a_{3,1,0} + ba_{2,1,1} + b^2a_{1,1,2} + b^3a_{0,1,3}, \\ a'_{2,2,0} &= a_{2,2,0} + ba_{1,2,1} + b^2a_{0,2,2}.\end{aligned} \tag{7.1}$$

All the valuations of the coefficients above are $\geq 1$ apart from $v(a_{2,2,0}) = 0$. Moreover, notice that $a'_{3,0,1}$ is the derivative in $b$ of $a'_{4,0,0}$. A necessary condition now is $p|Y$ and $p|Z$. Replacing $T$ by $\frac{1}{p}T(X, pY, pZ)$, we obtain the following triangle of valuations:

$$\begin{array}{cccccccc} Z^4 & \geq 5 & & & & & \\ & \geq 3 & \geq 5 & & & & \\ & \geq 2 & \geq 3 & \geq 5 & & & \\ & \geq 1 & \geq 2 & \geq 3 & \geq 5 & & \\ X^4 & \geq 0 & \geq 1 & = 1 & \geq 3 & \geq 5 & Y^4 \end{array}$$

By primitivity a necessary condition is $v(c(X^4)) > 0$, where $c(X^4) = a'_{4,0,0}/p$. The following steps rely on the possible factorisations of $f(b) = \overline{a'_{4,0,0}/p} \in \mathbb{F}_p[b]$. If, for instance, $f$ has only one root $\hat{b}$ this would mean that we can at most lift just one specific point on the line $y = 0$, the one which had initial coordinates $[1 : 0 : \hat{b}]$. Therefore, if $f(b)$ has no roots in $\mathbb{F}_p$ then none of the double points on $y = 0$ lift. Otherwise, if $f(b)$ has at least one root, we need also to consider the coefficient $a'_{3,0,1}$, which is linked to $a'_{4,0,0}$, and we study the probability of solubility looking at both the coefficients together. If the valuation $v(c(X^4))$ is strictly positive we have, after dividing by $p$, the following triangle of valuations:

$$\begin{array}{cccccccc} Z^4 & \geq 4 & & & & & \\ & \geq 2 & \geq 4 & & & & \\ & \geq 1 & \geq 2 & \geq 4 & & & \\ & \geq 0 & \geq 1 & \geq 2 & \geq 4 & & \\ X^4 & \geq 0 & \geq 0 & = 0 & \geq 2 & \geq 4 & Y^4 \end{array}$$

If $v(c(X^3Z)) = 0$ (recall that $\overline{c(X^3Z)} = \overline{a'_{3,0,1}/p} = f'(b)$) we have a smooth conic times a line squared, and therefore have a smooth point to lift; otherwise, we have a binary monic quadratic form times a double line.

Recalling that $\overline{a'_{3,0,1}} = f'(b)$ is the derivative of $\overline{a'_{4,0,0}} = f(b)$, which has degree 3, we describe the probabilities that each of the cases above happens.

Considering $f(b) \in \mathbb{F}_p[x]$ as a random polynomial, we divide the $p^4$ possible polynomials $f(b)$ into three subsets as follows:

(i) $\exists b \in \mathbb{F}_p | f(b) = 0$ and $f'(b) \neq 0$, i.e. $f$ has a simple root: by the difference with the other cases we have $(4p^4 - p^3 - 4p^2 + p)/6$ cases.

(ii) $\forall b$ such that $f(b) = 0$ we have $f'(b) = 0$, then either $f$ is the null polynomial or it has only double roots, i.e. it is a square or a cube of a linear polynomial. There are $2p^2 - 2p + 1$ such cases. Below we count these cases per number of double points.

(iii) $\forall b \in \mathbb{F}_p$ $f(b) \neq 0$: $f$ is either a non-zero constant ($p - 1$ cases) or irreducible over $\mathbb{F}_p$ with degree 2 or 3 (respectively $(p-1)^2 p/2$ and $(p-1)\left(p^3 - p\right)/3$ cases). This leads to $(2p^4 + p^3 - 8p^2 + 11p - 6)/6$ cases.

In case $(iii)$ we have no solubility. In case $(i)$, which happens with probability $(4p^3 - p^2 - 4p + 1)/(6p^3)$, we have solubility 1.

In case $(ii)$ the quartic reduces to a double line times a binary quadratic

$$\overline{T} = X^2(X^2\overline{a'_{4,0,0}/p^2} + XY\overline{a'_{3,1,0}/p} + Y^2\overline{a'_{2,2,0}}), \tag{7.2}$$

with $\overline{a'_{2,2,0}} \neq 0$.

By primitivity we need to determine whether a $\mathbb{F}_p$-rational point on (7.2) with $x \neq 0$ lifts. Let $\Delta$ be the discriminant of the second factor and assume $p \neq 2$ (the case $p = 2$ being easy to treat separately). If $\Delta = 0$ the quadratic has a double root, which without loss of generality we may move to $y = 0$ (since $\overline{a'_{2,2,0}} \neq 0$ it is not at $x = 0$). If $\left(\frac{\Delta}{p}\right) = +1$ we have distinct roots over $\mathbb{F}_p$ at least one of which has $x \neq 0$ and so lifts; while if $\left(\frac{\Delta}{p}\right) = -1$ there are no roots in $\mathbb{F}_p$ and we do not have solubility.

Continuing with the unresolved case where $y = 0$ is a double root; we denote by $\mu$ the solubility of this stage. In the case of $f$ having one double root the triangle of valuations is At this stage we have a situation similar to the starting one, however due to

| | | | | | | |
|---|---|---|---|---|---|---|
| $Z^4$ | $\geq 4$ | | | | | |
| | $\geq 2$ | $\geq 4$ | | | | |
| | $\geq 1$ | $\geq 2$ | $\geq 4$ | | | |
| | $\geq 1$ | $\geq 1$ | $\geq 2$ | $\geq 4$ | | |
| $X^4$ | $\geq 1$ | $\geq 1$ | $= 0$ | $\geq 2$ | $\geq 4$ | $Y^4$ |

Table 7.2: Quartic with solubility $\omega_2$.

the increase of some valuations the solubilities of these two configurations are different. Indeed, when we apply the same method used above, the coefficient $a'_{4,0,0}$ has at most degree 2 in $b$ when reduced mod $p$ instead of 3, this leads to different probabilities. Also, by primitivity, for solubility we must be able to lift a double point on $y = 0$ (and not on $x = 0$, which includes the quadruple point).

Therefore, the solubility of this case is not $\omega_1$ but $\omega_2$, indeed this quartic satisfies the conditions in the Definition 7.3.5.

If $f$ has a triple root, assuming $p$ different from 2, the triangle of valuations would be the same of the one in table 7.2 apart from the first column, which would be

$$Z^4 \quad \geq 4 \quad \geq 2 \quad \geq 2 \quad \geq 1 \quad \geq 1 \quad X^4$$

and therefore the solubility in case would be $\chi_2$.

In the case $f$ is the null polynomial the triangle of valuations would be again different just in the first column, having valuations:

$$Z^4 \quad \geq 4 \quad \geq 3 \quad \geq 2 \quad \geq 1 \quad \geq 1 \quad X^4$$

and in this case the solubility would be $\chi_3$.

Now we need to work out the probability that starting from a quartic in case $(ii)$ we end up in this configuration. Since $f$ has degree at most 3 we can have at most one double root, and we need to understand the probability that $f$ have either 1 or $p$ (when $f(b)$ is identically zero) *singular* roots.

Let $R$ be the set of roots of $f$. $\#R = 1$ if $f$ is either a square or a cube of a linear equation ($2p(p-1)$ cases). $\#R = p$ if $f$ is identically zero.

Now we compute for each of the 2 possible cardinalities of $R$ what are the probabilities of solubility, insolubility or indefinite case (either probability $\omega_2$ in the case of $f$ being a square or $\chi_2$ in the case of $f$ being a cubic). The reduction is the one described above in (7.2), where $h(b) = \overline{a'_{4,0,0}/p^2}$ has degree at most 4, $g(b) = \overline{a'_{3,1,0}/p}$ has degree at most 2 and $\overline{a'_{2,2,0}}$ is constant and non-zero. Since $h$ and $g$ have random coefficients, which are independent and uniformly distributed over $\mathbb{F}_p$, it follows that the discriminant $\Delta(b) = g(b)^2 - 4h(b)\overline{a'_{2,2,0}}$ of the quadratic form in (7.2) has all its 5 coefficients uniformly distributed. It follows that we can apply Theorem 7.2.2 which implies that $\Delta(b_i)$ are uniformly and independently distributed when $b_i \in R$ and $\#R \leq 5$. We have solubility when $\Delta(b_i)$ is a non-zero quadratic residue for at least one element of $R$, we end up in the configuration with solubility $\omega_2$ if $\Delta(b_i)$ is not a non-zero quadratic residue for all $i$ but it assumes the value 0 at least once. We have that

$$\mathbb{P}\left(\left(\frac{\Delta(b_0)}{p}\right) = 1\right) = \frac{p-1}{2p} = \psi,$$

from which we have

| | $\#R=1$ |
|---|---|
| Solubility 1 | $\psi=\frac{p-1}{2p}$ |
| $\omega_2$ or $\chi_2$ | $1-2\psi=\frac{1}{p}$ |
| Solubility 0 | $\psi=\frac{p-1}{2p}$ |

It remains to study the case when $\#R=p$, here we need to study the probability that $\Delta(b)$ has a certain degree and leading coefficient, then we can use the Lemma 7.2.1. Using that the coefficients of $\Delta(b)$ are uniformly and independently distributed together with the Lemma 7.2.1 we have the following table.

| $\deg(\Delta)$ | $\mathbb{P}(\deg(\Delta)=t)$ | Solubility 1 | Solubility $\chi_3$ | Solubility 0 |
|---|---|---|---|---|
| 4 | $\frac{p-1}{p}$ | $\frac{2p^2-1}{2p^2}$ | $\frac{p+1}{4p^3}$ | $\frac{p-1}{4p^3}$ |
| 3 | $\frac{p-1}{p^2}$ | 1 | 0 | 0 |
| 2 | $\frac{p-1}{p^3}$ | $\frac{2p-1}{2p}$ | $\frac{1}{2p}$ | 0 |
| 1 | $\frac{p-1}{p^4}$ | 1 | 0 | 0 |
| 0 | $\frac{1}{p^4}$ | $\frac{p-1}{2p}$ | $\frac{1}{p}$ | $\frac{p-1}{2p}$ |

Table 7.3: Solubilities for $\deg(\Delta)\leq 4$.

Recall that $\omega_1$ is the probability that at least one of the double points on the line $y=0$ (but not the quadruple one $[0:0:1]$) lifts, summarizing all the information above we have:

$$\begin{aligned}\omega_1 =&\frac{4p^3-p^2-4p+1}{6p^3}+\\ &\frac{1}{p^4}\left[\frac{p-1}{p}\left(\frac{2p^2-1}{2p^2}+\frac{p+1}{4p^3}\chi_3\right)+\frac{p-1}{p^2}+\right.\\ &\frac{p-1}{p^3}\left(\frac{2p-1}{2p}+\frac{1}{2p}\chi_3\right)+\frac{p-1}{p^4}+\frac{1}{p^4}\left(\frac{p-1}{2p}+\frac{1}{p}\chi_3\right)+\\ &\left.(2p^2-2p)\left(\frac{p-1}{2p}+\frac{\omega_2}{2p}+\frac{\chi_2}{2p}\right)\right].\end{aligned}$$

□

Now, with similar techniques, we link $\omega_2$ to $\omega_3$ with a linear equation.

**Lemma 7.3.8.**

$$\omega_2 = \frac{2(p-1)p^4\omega_3 - p^2 + \left(p\left(p^2+p-3\right)+3\right)p^4 + ((p-1)p+2)\chi_3 - 1}{2p^7}$$

*Proof.* In order to compute the probability of solubility $\omega_2$ we iterate the same procedure of the proof of the Lemma 7.3.7, the change of coordinates will give us the coefficients described in (7.1) with different valuations with respect Table 7.1, indeed all the coefficients of monomials that have exactly a factor $x$ have valuations at least 2, the ones who have no factor $x$ have valuations at least 4. Notice that now we can lift any point on the line $y = 0$ apart from $[1 : 0 : 0]$, independently on what happened at the previous step. Therefore, we consider again the change of coordinates that sends the point we want to lift to $[0 : 0 : 1]$ in order to study the behaviour of the coefficients. Since the procedure is really similar to the previous one we keep the same names for the polynomials describing the coefficients after the changes of variables even though they are different (basically they are made by different $p$-adic digits of the coefficients of the quartic $T$). In particular $f(b) = a'_{4,0,0}/p \bmod p$ has degree at most 2 and $h(b) = a'_{4,0,0}/p^2 \bmod p$ has degree at most 3. Similarly to the previous procedure, the first step is substitute $Y = pY'$ and $Z = pZ'$, and we consider the coefficient of $X^4$, whose reduction mod $p$ is $f(b)$. A necessary condition is $f(b) = 0$, at the next step we look at $f'(b)$, the reduction of $a'_{3,0,1}/p$, and if it is different from zero we have solubility. Let us look at the possible cases over a total of $p^3$ possibilities:

(i) $\exists b \in \mathbb{F}_p | f(b) = 0$ and $f'(b) \neq 0$, this happens if either $f$ has degree 1 ($p(p-1)$ cases) or has degree 2 and two distinct roots ($p(p-1)^2/2$ cases), it total there are $(p^3-p)/2$ cases.

(ii) $\forall b$ such that $f(b) = 0$ we have $f'(b) = 0$, so either $f$ is the null polynomial or is a square then we have $p^2 - p + 1$ cases.

(iii) $\forall b \in \mathbb{F}_p f(b) \neq 0$, $f$ is either a not zero constant or an irreducible quadratic, $(p^3 - 2p^2 + 3p - 2)/2$ cases.

We have solubility in case $(i)$ with probability $(p^2-1)/2p^2$ and we continue our investigation in case $(ii)$.

If $f$ is a square there exists only a $\hat{b}$ such that $f(\hat{b}) = 0$, therefore the discriminant $\Delta(\hat{b})$ of the quadratic in the reduction is a constant, which is a non-zero quadratic residue with probability $(p-1)/2p$ (in this case we have two different roots and hence solubility)

or 0 with probability $1/p$ and then, moving the double root to $y = 0$, we end up in the configuration:

$$\begin{array}{cccccc} Z^4 & \geq 6 & & & & \\ & \geq 3 & \geq 6 & & & \\ & \geq 1 & \geq 3 & \geq 6 & & \\ & \geq 1 & \geq 1 & \geq 3 & \geq 6 & \\ X^4 & \geq 1 & \geq 1 & = 0 & \geq 3 & \geq 6 \quad Y^4 \end{array}$$

Table 7.4: Quartic with solubility $\omega_3$.

The solubility of this case is $\omega_3$. When $f(b)$ is identically zero (probability $1/p^3$) the reduction of the quartic is a double line times a quadratic binary equation, as above $\Delta(b)$ is the discriminant of the quadratic. In particular the triangle of valuations will be the same as in Table 7.4 a part from the first column, where we would have

$$Z^4 \quad \geq 8 \quad \geq 4 \quad \geq 2 \quad \geq 1 \quad \geq 1 \quad X^4$$

and therefore the solubility in case would be $\chi_3$. We have that $h(b)$, the reduction of $a'_{4,0,0}/p^2 \bmod p$, has at most degree 3 and its coefficients are uniformly distributed, moreover $g(b) = \overline{a'_{3,1,0}/p}$ has degree at most 1, therefore the coefficients of $\Delta(b) = g(b)^2 - 4h(b)\overline{a'_{2,2,0}}$ are uniformly and independently distributed over $\mathbb{F}_p$ since $\overline{a'_{2,2,0}} \neq 0$. By the Lemma 7.2.1 we have:

| $\deg(\Delta)$ | $\mathbb{P}(\deg(\Delta) = t)$ | Solubility 1 | Solubility $\chi_3$ | Solubility 0 |
|---|---|---|---|---|
| 3 | $\frac{p-1}{p}$ | 1 | 0 | 0 |
| 2 | $\frac{p-1}{p^2}$ | $\frac{2p-1}{2p}$ | $\frac{1}{2p}$ | 0 |
| 1 | $\frac{p-1}{p^3}$ | 1 | 0 | 0 |
| 0 | $\frac{1}{p^3}$ | $\frac{p-1}{2p}$ | $\frac{1}{p}$ | $\frac{p-1}{2p}$ |

Table 7.5: Solubilities for $\deg(\Delta) \leq 3$.

From this it follows that:

$$\begin{aligned} \omega_2 =& \frac{(p^2-1)}{2p^2} + \frac{p-1}{p^2}\left(\frac{p-1}{2p} + \frac{\omega_3}{p}\right) + \\ & \frac{1}{p^3}\left[\left(\frac{p-1}{p} + \frac{p-1}{p^2}\left(\frac{2p-1}{2p} + \frac{\chi_3}{2p}\right) + \frac{p-1}{p^3} + \frac{1}{p^3}\left(\frac{p-1}{2p} + \frac{\chi_3}{p}\right)\right)\right]. \end{aligned}$$

□

If we keep expressing $\omega_k$ in function of $\omega_{k+1}$ we would never finish but, luckily the next one is the last step. Indeed, by the proposition we have that all the $\omega_k$, for $k \geq 3$, are equal.

**Lemma 7.3.9.**

$$\omega_k = \frac{p^6 + p^5 - 3p^4 + 3p^3 - p^2 - 1 + \chi_3(p^2 - p + 2)}{2p^6 - 2p^4 + 2p^3}$$

*for all* $k \geq 3$.

*Proof.* We want to evaluate $\omega_3$, by deriving a recursive formula. After we change the coordinates mapping one of the points of $y = 0$ different from $[0 : 0 : 1]$ to $[1 : 0 : 0]$ the coefficients will be as in (7.1) but with different valuations with respect to the case of $\omega_2$: all the coefficients of monomials that have at most a factor $x$ (i.e they do not have $x^2$ or higher) have valuations at least 3, therefore during the procedure those coefficients will not affect the reduction since we divide by $p$ just twice. In particular $f(b) = \overline{a'_{4,0,0}/p}$ has degree at most 2 and $h(b) = \overline{a'_{4,0,0}/p^2}$ as well. We substitute $Y = pY'$ and $Z = pZ'$, we end up again to look at the coefficient of $X^4$, whose reduction mod $p$ is $f(b)$. A necessary condition is $f(b) = 0$, at the next step we look at $f'(b)$, the reduction of $a'_{3,0,1}/p$, and if it will be different to zero we have solubility. We have already studied all possible cases, we have solubility in case $(i)$ with probability $(p^2 - 1)/2p^2$ and we continue our investigation in case $(ii)$. If $f$ is a square there exists only a $\hat{b}$ such that $f(\hat{b}) = 0$. Therefore, the discriminant $\Delta(\hat{b})$ of the quadratic in the reductions is a constant: it is a non-zero quadratic residue with probability $(p - 1)/2p$ (which give us two different roots, and so we have solubility) or 0 with probability $1/p$. In the latter case, moving the double root to $y = 0$, we end up in the configuration: which has probability of solubility

| | | | | | | |
|---|---|---|---|---|---|---|
| $Z^4$ | $\geq 8$ | | | | | |
| | $\geq 4$ | $\geq 8$ | | | | |
| | $\geq 1$ | $\geq 4$ | $\geq 8$ | | | |
| | $\geq 1$ | $\geq 1$ | $\geq 4$ | $\geq 8$ | | |
| $X^4$ | $\geq 1$ | $\geq 1$ | $= 0$ | $\geq 4$ | $\geq 8$ | $Y^4$ |

Table 7.6: Quartic with solubility $\omega_3$.

$\omega_3$. Indeed, all the following reductions we would apply, and in particular the polynomial $f(b)$ and $h(b)$, have the same properties and valuations of the previous one. Although the valuations of the coefficients of the monomials with at most a factor $x$ increase at each step they do not affect the probability of solubility, since this recursive method does

not rely on those specific coefficients.

From this observation follows that $\omega_k = \omega_{k+1}$ for all $k \geq 3$.

If the polynomial $f(b)$ is identically zero (probability $1/p^3$) we do not have any information on $h(b)$, the reduction of $a'_{4,0,0}/p^2$ mod $p$, and $b$ has not been fixed yet. In particular the triangle of valuations will be the same as in Table 7.6 a part from the first column, where we would have

$$Z^4 \quad \geq 8 \quad \geq 4 \quad \geq 2 \quad \geq 1 \quad \geq 1 \quad X^4$$

and therefore the solubility in case would be $\chi_3$. Let us understand what happens to the discriminant of the quadratic $\Delta(b)$, whose 3 coefficients are uniformly distributed since the coefficients of $h$ are uniformly distributed as well. By Lemma 7.2.1 we have the Table 7.3.

| $\deg(\Delta)$ | $\mathbb{P}(\deg(\Delta) = t)$ | Solubility 1 | Solubility $\chi_3$ | Solubility 0 |
|---|---|---|---|---|
| 2 | $\frac{p-1}{p}$ | $\frac{2p-1}{2p}$ | $\frac{1}{2p}$ | 0 |
| 1 | $\frac{p-1}{p^2}$ | 1 | 0 | 0 |
| 0 | $\frac{1}{p^2}$ | $\frac{p-1}{2p}$ | $\frac{1}{p}$ | $\frac{p-1}{2p}$ |

Table 7.7: Solubilities for $\deg(\Delta) \leq 2$.

Summarising we have:

$$\begin{aligned}\omega_3 =& \frac{(p^2-1)}{2p^2} + \frac{p-1}{p^2}\left(\frac{p-1}{2p} + \frac{\omega_3}{p}\right) + \\ & \frac{1}{p^3}\left[\left(\frac{p-1}{p}\left(\frac{2p-1}{2p} + \frac{\chi_3}{2p}\right) + \frac{p-1}{p^2} + \frac{1}{p^2}\left(\frac{p-1}{2p} + \frac{\chi_3}{p}\right)\right)\right].\end{aligned}$$

□

We now compute the solubilities $\chi_2$ and $\chi_3$ defined in 7.3.6.

**Lemma 7.3.10.**

$$\chi_2 = \frac{2p^6 - 2p^5 + 2p^4 + p^2\chi_3 - p^2 - p\chi_3 + 2\chi_3 - 1}{2p^6}.$$

*Proof.* We want to evaluate $\chi_2$ in function of the solubility $\chi_3$. After we change the coordinates mapping one of the points of $y = 0$ different from $[0 : 0 : 1]$ to $[1 : 0 : 0]$ the coefficients will be as in (7.1). We have that $f(b) = \overline{a'_{4,0,0}/p}$ has degree at most 1

and $h(b) = \overline{a'_{4,0,0}/p^2}$ has degree at most 3. We substitute $Y = pY'$ and $Z = pZ'$, we end up again to look at the coefficient of $X^4$, whose reduction mod $p$ is $f(b)$. A necessary condition is $f(b) = 0$, at the next step we look at $f'(b)$, the reduction of $a'_{3,0,1}/p$, and if it will be different to zero we have solubility. We have already studied all possible cases, we have solubility in case $(i)$ with probability $(p-1)/p$ and we continue our investigation in case $(ii)$, when $f$ is the null polynomial, which happens with probability $1/p^2$. If the polynomial $f(b)$ is identically zero we do not have any information on $h(b)$, the reduction of $a'_{4,0,0}/p^2$ mod $p$, and $b$ has not been fixed yet. In the case the quadratic is a square we end up, after moving the double root to $y = 0$ to this configuration:

$$\begin{array}{cccccc} Z^4 & \geq 6 & & & & \\ & \geq 3 & \geq 6 & & & \\ & \geq 2 & \geq 3 & \geq 6 & & \\ & \geq 1 & \geq 1 & \geq 3 & \geq 6 & \\ X^4 & \geq 1 & \geq 1 & = 0 & \geq 3 & \geq 6 \quad Y^4 \end{array}$$

which has probability of solubility $\chi_3$.

Let us understand what happens to the discriminant of the quadratic $\Delta(b)$, whose 4 coefficients are uniformly distributed since the coefficients of $h$ are uniformly distributed as well. By Lemma 7.2.1 we have the Table 7.3.

| $\deg(\Delta)$ | $\mathbb{P}(\deg(\Delta) = t)$ | Solubility 1 | Solubility $\chi_3$ | Solubility 0 |
|---|---|---|---|---|
| 3 | $\frac{p-1}{p}$ | 1 | 0 | 0 |
| 2 | $\frac{p-1}{p^2}$ | $\frac{2p-1}{2p}$ | $\frac{1}{2p}$ | 0 |
| 1 | $\frac{p-1}{p^3}$ | 1 | 0 | 0 |
| 0 | $\frac{1}{p^3}$ | $\frac{p-1}{2p}$ | $\frac{1}{p}$ | $\frac{p-1}{2p}$ |

Table 7.8: Solubilities for $\deg(\Delta) \leq 3$.

From this it follows that:

$$\chi_2 = \frac{(p-1)}{p} + \frac{1}{p^2}\left[\left(\frac{p-1}{p} + \frac{p-1}{p^2}\left(\frac{2p-1}{2p} + \frac{\chi_3}{2p}\right) + \frac{p-1}{p^3} + \frac{1}{p^3}\left(\frac{p-1}{2p} + \frac{\chi_3}{p}\right)\right)\right].$$

□

**Lemma 7.3.11.**

$$\chi_3 = \frac{2p^4 + 2p^2 + p + 1}{2p^4 + 2p^3 + 2p^2 + p + 2},$$

*for all* $k \geq 3$.

*Proof.* We want to evaluate $\chi_3$, by deriving a recursive formula. After we change the coordinates mapping one of the points of $y = 0$ different from $[0 : 0 : 1]$ to $[1 : 0 : 0]$ the coefficients will be as in (7.1) but with different valuations with respect to the case of $\chi_2$; in particular $f(b) = \overline{a'_{4,0,0}/p}$ has degree at most 1 and $h(b) = \overline{a'_{4,0,0}/p^2}$ has degree at most 2. We substitute $Y = pY'$ and $Z = pZ'$, we end up again to look at the coefficient of $X^4$, whose reduction mod $p$ is $f(b)$. A necessary condition is $f(b) = 0$, at the next step we look at $f'(b)$, the reduction of $a'_{3,0,1}/p$, and if it will be different to zero we have solubility. We have already studied all possible cases, we have solubility in case $(i)$ with probability $(p-1)/p$ and we continue our investigation in case $(ii)$, when $f$ is the null polynomial, which happens with probability $1/p^2$. If the polynomial $f(b)$ is identically zero we do not have any information on $h(b)$, the reduction of $a'_{4,0,0}/p^2$ mod $p$, and $b$ has not been fixed yet. In the case the quadratic is a square we end up, after moving the double root to $y = 0$ to this configuration:

$$\begin{array}{cccccccc}
Z^4 & \geq 6 & & & & & \\
 & \geq 4 & \geq 6 & & & & \\
 & \geq 2 & \geq 3 & \geq 6 & & & \\
 & \geq 1 & \geq 1 & \geq 3 & \geq 6 & & \\
X^4 & \geq 1 & \geq 1 & = 0 & \geq 3 & \geq 6 & Y^4
\end{array}$$

which has probability of solubility $\chi_3$. Indeed, all the following reductions we would apply, and in particular the polynomial $f(b)$ and $h(b)$, have the same properties and valuations of the previous one. Although the valuations of the coefficients of the monomials with at most a factor $x$ increase at each step they do not affect the probability of solubility, since this recursive method does not rely on those specific coefficients.

From this observation follows that $\chi_k = \chi_{k+1}$ for all $k \geq 3$.

Let us understand what happens to the discriminant of the quadratic $\Delta(b)$, whose 3 coefficients are uniformly distributed since the coefficients of $h$ are uniformly distributed as well. By Lemma 7.2.1 we have the Table 7.3.

Summarising we have:

$$\chi_3 = \frac{(p-1)}{p} + \frac{1}{p^2}\left[\left(\frac{p-1}{p}\left(\frac{2p-1}{2p} + \frac{\chi_3}{2p}\right) + \frac{p-1}{p^2} + \frac{1}{p^2}\left(\frac{p-1}{2p} + \frac{\chi_3}{p}\right)\right)\right].$$

| $\deg(\Delta)$ | $\mathbb{P}(\deg(\Delta)=t)$ | Solubility 1 | Solubility $\chi_3$ | Solubility 0 |
|---|---|---|---|---|
| 2 | $\frac{p-1}{p}$ | $\frac{2p-1}{2p}$ | $\frac{1}{2p}$ | 0 |
| 1 | $\frac{p-1}{p^2}$ | 1 | 0 | 0 |
| 0 | $\frac{1}{p^2}$ | $\frac{p-1}{2p}$ | $\frac{1}{p}$ | $\frac{p-1}{2p}$ |

Table 7.9: Solubilities for $\deg(\Delta) \leq 2$.

□

Gathering together the information from the previous lemmas we obtain the expressions of $\omega_1$ and $\omega_2$ as rational functions in $p$.

**Corollary 7.3.12.** *Substituting the value of $\chi_3$ from Lemma 7.3.11 in the formula of Lemma 7.3.10 we have*

$$\chi_2 = \frac{2p^7+2p^5+p^4+3p^3-3p^2+3p-2}{2p^7+2p^6+2p^5+p^4+2p^3},$$

*and substituting the same value in Lemma 7.3.9 we have*

$$\omega_3 = \frac{2p^7+4p^6-2p^5+3p^4+3p^3+p^2-p+2}{4p^7+4p^6+2p^4+4p^3+2p^2-2p+4}.$$

*We can now compute from the formula of Lemma* 7.3.8 *the expression of $\omega_2$*

$$\omega_2 = \frac{2p^{11}+4p^{10}-2p^9+3p^8+3p^7+5p^6-7p^5+4p^4+6p^3-12p^2+10p-4}{4p^{11}+4p^{10}+2p^8+4p^7+2p^6-2p^5+4p^4}.$$

*Then, using the formula of Lemma 7.3.7, we obtain $\omega_1$, whose numerator is:*

$$32p^{20}+24p^{19}+8p^{18}+16p^{17}+12p^{16}+40p^{15}+66p^{14}-44p^{13}-60p^{12}+105p^{11}+17p^{10}$$
$$-198p^9+282p^8-255p^7+201p^6-108p^5-72p^4+228p^3-258p^2+156p-48,$$

*and its denominator is*

$$24p^{13}\left(p\left(p(p+1)\left(2p^4+p+1\right)-1\right)+2\right).$$

Now, we are ready to face the probability of solubility of a point having a double tangent.

**Proposition 7.3.13.** *Let $T$ be a ternary homogeneous quartic over $\mathbb{Q}_p$. If its reduction $\overline{T}$ contains a singular point $P$ with a double tangent then the probability that $P$ lifts to a point over $\mathbb{Q}_p$ is*

$$\frac{2p^2 - p + 2\omega_1 - 1}{2p^3},$$

*where $\omega_1$ is defined in 7.3.5 and its value is stated in Corollary 7.3.12.*

*Proof.* We move the singular point $P$ to $[1:0:0]$, then the reduction of $T$ is

$$\overline{T} := x^2L^2 + xC_3 + C_4,$$

where $L$ is the double $\mathbb{F}_p$-tangent to $\overline{T}$ at $P$ and the $C_i$'s are forms of degree $i$ in $y$ and $z$. In order to lift $P$, we substitute $Y$ with $pY$ and $Z$ with $pZ$ in $T$; and dividing by $p$ we obtain

$$\overline{T} := ux^4.$$

Since the $x$-coordinate of $P$ is not zero its lift cannot neither be zero, therefore $u$ has to be zero, which corresponds to the first $p$-adic digit of $a_{4,0,0}$. This happens with probability $1/p$. Assuming $u = 0$ we can divide again by $p$ and obtain

$$\overline{T} = x^2(ux^2 + vxy + wxz + L^2) = x^2\gamma.$$

Since the intersection between the conic defined by $\gamma$ and $x = 0$ is a double point there are no restrictions on the type of the conic $\gamma$. We can assume $L = y$ and then after replacing[2] $y$ with $y - (v/2)x$, in this way $v = 0$. Therefore, the reduction is now

$$\overline{T} = x^2(ux^2 + wxz + y^2).$$

If $w \neq 0$, which happens with probability $\frac{p-1}{p}$, the conic is irreducible and therefore we have smooth points to lift. If $w = 0$ and $u = 0$, which happens with probability $\frac{1}{p^2}$, the reduction is a product of 2 lines squared where we need to work further to compute the solubility. If $w = 0$ and $u \neq 0$, probability equal to $\frac{p-1}{p^2}$, then the reduction is a product of two lines. Those lines either are conjugate if $-u$ is not a square in $\mathbb{F}_p$, which happens with probability $\frac{1}{2}$, or are two distinct lines over $\mathbb{F}_p$, with relative probability $\frac{1}{2}$. In the first case we have no solubility, in the latter there are smooth points to lift.

It remains to deal with the only undetermined case: the product of two lines

[2]This substitution is defined when the characteristic is not 2. Actually the method works even for characteristic equal to 2, but in order to simplify the exposition we describe just the case with odd characteristic.

squared. The computation of the probability of solubility of this case has been studied in the previous lemmas. Indeed, changing the coordinates in such a way the second double line is $y = 0$, the triangle of valuations of the coefficients is:

$$\begin{array}{cccccc} Z^4 & \geq 2 & & & & \\ & \geq 1 & \geq 2 & & & \\ & \geq 1 & \geq 1 & \geq 2 & & \\ & \geq 1 & \geq 1 & \geq 1 & \geq 2 & \\ X^4 & \geq 1 & \geq 1 & = 0 & \geq 1 & \geq 2 \quad Y^4 \end{array}$$

and we cannot lift points that are on $x = 0$. Therefore, by definition, the solubility of this case is $\omega_1$.

□

We are now ready to compute the probability of solubility of a double point over the reduction of a quartic curve.

**Proposition 7.3.14** (Solubility of a double point)**.** *Let $P$ be a singular double point on the reduction of a quartic curve. The probability that it will lift to a point over $\mathbb{Q}_p$ is*

$$\frac{2p^5 + 3p^4 + 4p^3 + 2p^2\omega_1 - p^2 + 4p\omega_1 - 3p + 2\omega_1 - 1}{2p^3(p^3 + 2p^2 + 2p + 1)},$$

*where $\omega_1$ is formulated in the proof of Proposition* 7.3.13*, its numerator is*

$$\begin{aligned} &32p^{20} + 24p^{19} + 8p^{18} + 16p^{17} + 12p^{16} + 40p^{15} + 66p^{14} - 44p^{13} - 60p^{12} + 105p^{11} + 17p^{10} \\ &- 198p^9 + 282p^8 - 255p^7 + 201p^6 - 108p^5 - 72p^4 + 228p^3 - 258p^2 + 156p - 48, \end{aligned}$$

*and its denominator is*

$$24p^{13}\left(p\left(p(p+1)\left(2p^4 + p + 1\right) - 1\right) + 2\right).$$

*Proof.* We move the singular point to $[0 : 0 : 1]$, so the reduction has equation

$$\overline{T} := z^2C_2 + zC_3 + C_4,$$

where $C_2$ is a non-null quadratic in $x$ and $y$. In order to compute the solubility of the general case we need to work out the probability of each configuration. The possible configurations are encoded in the type of factorisation of $C_2$. There are in total $p^3 - 1$ non-zero quadric binary equations, and they divide as follows:

- $\frac{p^3-p}{2}$ which split, i.e. two different tangent defined over $\mathbb{F}_p$;
- $\frac{p(p-1)^2}{2}$ which are irreducible on $\mathbb{F}_p$, so there are two conjugate tangents over $\mathbb{F}_{p^2}$;
- $p^2-1$ which are squares, with a double tangent.

Weighting the solubility of the three cases with the probability that a specific case happens we have the final formula:

$$\frac{1}{p^3-1}\left(\frac{p^2-1}{2}+\frac{p(p-1)^2}{2(p+1)}+(p^2-1)\frac{1}{p}\left(\frac{p-1}{p}+\frac{p-1}{2p^2}+\frac{\omega_1}{p^2}\right)\right)=$$

$$\frac{2p^5+3p^4+4p^3+2p^2\omega_1-p^2+4p\omega_1-3p+2\omega_1-1}{2p^3(p^3+2p^2+2p+1)}.$$

□

## 7.4 The undetermined semi-stable reductions

Between the undetermined cases the semi-stable ones are:

- Product of two conjugate conics whose $\mathbb{F}_p$-rational intersection points have intersection multiplicity 1.
- Product of two pairs of conjugate lines that do not have a quadruple $\mathbb{F}_p$-rational point of intersection.

Thanks to the local solubility results of the previous section we are able to compute the solubility of all the semi-stable reductions.

### 7.4.1 Product of two conjugate conics

In order to compute the probability of solubility when the reduction is the product of two conjugate conics we describe a model that will help our computation. Over $\mathbb{F}_p$, the number of $\mathbb{F}_p$-rational points of the product of conjugate conics is at most 4, this can be deduce from the fact that a $\mathbb{F}_p$-rational point is fixed by the Galois action, so all the $\mathbb{F}_p$ points are intersection points between the two conics, which consists in at most 4 points by the Bézout's theorem. These intersection points may differ in their multiplicities, and we will take into account this invariant in the computation of the solubility. We are interested in quartics which have at least one $\mathbb{F}_p$ point, which we move to $P=[0:0:1]$. Each conic has a tangent line at the point $P$, the two lines can be conjugate or equal

and so $\mathbb{F}_p$-rational; if they are equal we move them to the line $x = 0$. As described in detail in Section 5.2, if the tangent lines are distinct the multiplicity of the intersection is 1, otherwise it is at least 2. Since this section is dedicated to the semi-stable reductions here we describe just the cases when the tangent lines are conjugate.

**One $\mathbb{F}_p$ point with intersection multiplicity 1**

As said above we move the point of intersection to $P = [0 : 0 : 1]$ and the tangent lines are distinct, this leads us to the reduction on $\mathbb{F}_p$ which factors over $\mathbb{F}_{p^2}$ as

$$\overline{T} = (Q(x, y) + zL(x, y))(\sigma(Q) + z\sigma(L)),$$

where $L$ and $\sigma(L)$ are the tangent lines at $P$ respectively for the two conjugate conics and $\sigma$ is the Frobenius endomorphism. Applying the result from Proposition 7.3.2, since we have just one singular point, the total solubility here is $\frac{1}{p+1}$.

**Two $\mathbb{F}_p$ points both with intersection multiplicity 1**

We can move one singular point to $[1 : 0 : 0]$ and the other to $[0 : 0 : 1]$, then we apply the methods described in Proposition 7.3.2 and notice that the conditions on the valuations refer to two disjoint sets of coefficients (respectively $a_{4,0,0}$ and $a_{0,0,4}$), therefore their probability of solubility are equal and independent. Then the total solubility in this case is

$$1 - (1 - \frac{1}{p+1})^2 = \frac{2p+1}{p^2+2p+1}.$$

**Four $\mathbb{F}_p$ points, all with intersection multiplicity 1**

We can move the four singular points to $[1 : 0 : 0]$, $[0 : 1 : 0]$, $[0 : 0 : 1]$ and $[1 : 1 : 1]$. Then, if we apply the methods described in Proposition 7.3.2, is clear that the first three points have independent solubilities since the conditions are imposed on disjoint sets of coefficients (respectively $a_{4,0,0}$, $a_{0,4,0}$ and $a_{0,0,4}$), but what about the fourth point? Would it be possible to reformulate its solubility condition in order to understand the dependency on the solubility of the other singular points? Although it was not immediately clear that the liftability of the four points were independent, extensive numerical experiments suggested that they are, following which we found the following proof.

Indeed, we can swap the two singular points $[1:0:0]$ and $[1:1:1]$ by

$$\begin{aligned} x' &= x \\ y' &= x - y \\ z' &= x - z. \end{aligned}$$

Now, the coefficient of $X^4$ is given by the sum of all coefficients $a'_{4,0,0} = \sum a_{i,j,k}$. In particular $a_{2,1,1}$ is one of the terms of the sum and it is independent of all the other coefficients and conditions imposed to determine the liftability of the other 3 singular points, indeed just its zero digit was involved in the procedure, which is determined by the type of reduction. Therefore also in this case we can rewrite the condition of solubility independently of the other coefficients and therefore, the total solubility in this case is

$$1 - (1 - \frac{1}{p+1})^4 = \frac{4p^3 + 6p^2 + 4p + 1}{(p+1)^4}.$$

### 7.4.2 Two pairs of conjugate lines without quadruple point

Two pairs of conjugate lines may occur in basically two different configurations: either with just one intersection point of order 4 or with 6 intersection points of order 2, of which two are $\mathbb{F}_p$-rational. Since we want to describe all the semi-stable reductions first, here we only consider the latter case. Therefore, we want to compute the probability that any of the two singular points would lift. Those points have conjugate tangents (actually they are the lines defining the reduction), so we can compute their solubility just by their local condition, using the formula in Proposition 7.3.2. As in Paragraph 7.4.1 we can map the two points to $[1:0:0]$ and $[0:1:0]$ and conclude that the two solubility are independent. In conclusion the probability of solubility in this case is

$$\frac{2p+1}{p^2+2p+1}.$$

# Chapter 8

# Solubility of non-semistable reductions

In order to compute the probability of solubility of a generic plane quartic defined over $\mathbb{Q}_p$ we look at its reduction over $\mathbb{F}_p$. In the previous chapter we have studied the cases where the reduction is semistable. We still have to deal with the non-semistable reductions: they may have multiple components and/or singular points that are not nodal. In this chapter we discuss the solubility of those reductions. In certain cases we are able to deduct a closed formula, while in others we are only able to derive an estimate with lower and upper bounds.

## 8.1 Auxiliary reductions

Before we deal with the standard reductions we describe some particular ones that appear quite often during the computation of the probability of solubilities of the standard cases.

**Proposition 8.1.1.** *Let $\overline{T}$ be the reduction over $\mathbb{F}_p$ of a quartic defined over $\mathbb{Z}_p$. Let $\overline{T}$, up to change of variables, have equation*

$$\overline{T} = z^2(x^2 + axz + bz^2),$$

*with $a$ and $b$ uniform in $\mathbb{F}_p$. Together with the additional conditions $v(a_{0,2,2}) = 1$, $v(a_{0,3,1}) \geq 2$ and $v(a_{0,4,0}) \geq 2$. Then the probability of lifting any point not in the line $z = 0$ is $\frac{1}{2}$.*

*Proof.* Let $\tau$ be the probability of solubility of this specific reduction. The triangle of valuations is the following;

$$\begin{array}{cccccc} Z^4 & \geq 0 & & & & \\ & \geq 0 & \geq 1 & & & \\ & = 0 & \geq 1 & = 1 & & \\ & \geq 1 & \geq 1 & \geq 1 & \geq 2 & \\ X^4 & \geq 1 & \geq 1 & \geq 1 & \geq 1 & \geq 2 \quad Y^4 \end{array}$$

The equation of the reduction $\overline{T}$ has the form $z^2(x^2 + axz + bz^2)$. Any rational point $(X : Y : Z)$ on $T$ with $p \nmid Z$ comes from lifting a root of the binary quadratic factor $(x^2 + axz + bz^2)$. The binary quadratic can have one of the following sets of roots:

- two conjugate roots (with probability $(p-1)/2p$), but this would imply $p|Z$, so in this case we cannot lift any point;
- a double root (with probability $1/p$);
- two $\mathbb{F}_p$-rational roots (with probability $(p-1)/2p$), then we can lift them (since they cannot have the $z$-coordinate equal to 0).

The only undetermined case is the second one. Since the coefficients of $x^2$ is not null we cannot have $z = 0$ as double root. After a change of coordinates that sends the double line to $x = 0$ we have $\overline{T} = z^2x^2$. We can substitute $X$ with $pX$ and divide everything by $p$, which give us the following triangle of valuations:

$$\begin{array}{cccccc} Z^4 & \geq 0 & & & & \\ & \geq 1 & \geq 0 & & & \\ & = 1 & \geq 1 & = 0 & & \\ & \geq 3 & \geq 2 & \geq 1 & \geq 1 & \\ X^4 & \geq 4 & \geq 3 & \geq 2 & \geq 1 & \geq 1 \quad Y^4 \end{array}$$

By the initial conditions on the coefficients of $y^3z$ and $y^4$ these terms do not appear in the reduction of $T$ at this stage. Now, the reduction has the form $z^2(y^2 + cyz + dz^2)$, and all the side conditions are fulfilled (just swapping $x$ and $y$) so the solubility is the same. Therefore, the probability of solubility $\tau$ is described recursively by

$$\tau = \frac{p-1}{2p} + \frac{1}{p}\tau$$

which implies $\tau = 1/2$. □

Now we consider a quite common reduction. A double line times a conic with some side condition: the intersection between conic and double line are two conjugate points. In particular, we are interested in lifting points that are not on the double line.

**Proposition 8.1.2.** *Let $\overline{T}$ be the reduction over $\mathbb{F}_p$ of a quartic defined over $\mathbb{Z}_p$. If $\overline{T} = 0$ is the locus of a double line together with a conic and the intersection between the conic and the double line are two conjugate points; then the probability of lifting any point not on the double line in $\mathbb{P}^2(\mathbb{F}_p)$ is $\frac{p}{p+1}$.*

*Proof.* Let $\tau$ be the probability of solubility of this reduction. We move without loss of generality the double line to $x = 0$. Then, the reduction is

$$\overline{T} = x^2(C_2(y,z) + xC_1(y,z) + x^2C_0(y,z)) = x^2\gamma.$$

When we intersect the conic $\gamma$ with the line $x = 0$ we got two conjugate points, therefore $\gamma$ could be either an irreducible conic or a product of two conjugate lines whose intersection point is not in the line $x = 0$. Let us compute the probabilities of each case. The intersection between $\gamma = 0$ and $x = 0$ is described by $C_2(y,z) = 0$, which has to be irreducible over $\mathbb{F}_p$ in order to have two conjugate points of intersection. The total number of the possible cases is $p^3(p^2-p)/2$. The two possible reductions are:

(i) two conjugate lines whose intersection is not on the line $x = 0$, with probability equal to $\frac{p^4-p^3}{p^5-p^4} = \frac{1}{p}$;

(ii) a smooth conic, where we do have a smooth point to lift, with probability equal to $\frac{p^5-2p^4+p^3}{p^5-p^4} = \frac{p-1}{p}$.

The probabilities above can be computed by simple combinatorics arguments on the factorisation of $\gamma$. The only case where we still have to determine the solubility is the product of two conjugate lines. Since there is just one possible point to lift the probability is described by Proposition 7.3.2, ad it is equal to $\frac{1}{p+1}$. Therefore the overall probability of solubility is

$$\tau = \frac{1}{p(p+1)} + \frac{p-1}{p} = \frac{p}{p+1}.$$

□

The following proposition gives us a result that will be useful when a particular side condition is known about the quartic: the reduction is a binary quartic with no

roots over $\mathbb{F}_p$. It occurs, for instance, when the reduction is a union of 4 conjugate lines over $\mathbb{F}_{p^4}$ or when there are two conjugate lines over $\mathbb{F}_{p^2}$ squared. What we will really use about this side condition is that the valuation of certain coefficients does not vary by any $\mathbb{F}_p$-rational change of coordinates.

**Proposition 8.1.3.** *Let a quartic $T$ defined over $\mathbb{Z}_p$ be $X^2C_2(X,Y,Z)+pXC_3(X,Y,Z)+pC_4(Y,Z))$, where the reduction $\overline{C_4}(y,z)$ has no roots over $\mathbb{F}_p$, $v(C_2)=0$. Assuming that we cannot lift the points on the line $x=0$ the probability of solubility is*

$$p\big(8p^{13}+20p^{12}+36p^{11}+45p^{10}+59p^9 \\ +68p^8+67p^7+69p^6+68p^5+56p^4+48p^3+36p^2+24p+8\big)$$

*divided by*

$$8(p+1)^2\left(p^2-p+1\right)\left(p^2+p+1\right)^2\left(p^6+p^3+1\right).$$

*Proof.* Let us consider the reduction of the quartic $\overline{T}=x^2\overline{C_2}(x,y,z)$. The conic $\overline{C_2}(x,y,z)$ can have one of the following factorisations:

- a line squared different from $x=0$, which happens with probability $\frac{p(p^2-1)}{p^6-1}$;
- two conjugate lines whose intersection is not on the line $x=0$, which happens with probability $\frac{p^3(p-1)^2}{2(p^6-1)}$;
- $x^2=0$, which happens with probability $\frac{p-1}{p^6-1}$. In this case, by primitivity of $C_2$, we have no solubility;
- two conjugate lines whose intersection is on the line $x=0$, which happens with probability $\frac{p^2(p-1)^2}{2(p^6-1)}$. In this case, by primitivity, we have no solubility;
- two distinct $\mathbb{F}_p$-lines, which happens with probability $\frac{p^4+2p^3+2p^2+p}{2(p^5+p^4+p^3+p^2+p+1)}$. In this case there is at least one smooth point to lift;
- A smooth conic,which happens with probability $\frac{p^5-p^2}{p^5+p^4+p^3+p^2+p+1}$. Here again we have a smooth point to lift.

The only cases where we should keep investigating are the first two.

**Two conjugate lines case.**

In the case the reduction $\overline{C_2}$ is two conjugate lines, we assume without loss of generality that $\overline{C}=(y+\delta z)(y+\sigma(\delta)z)$, where $\sigma$ is the Frobenius of $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$. This forces $p|Y$ and $p|Z$. After the substitution $T\to T(X,pY,pZ)/p$ we have $\overline{T}=ax^4$,

by primitivity $x \neq 0$, then we can continue if and only if $a = 0$, which happens with probability $1/p$. Then, dividing by $p$, we obtain

$$\overline{T} = x^2 \left( (y + \delta z)(y + \sigma(\delta) z) + x C_1(y, z) + x^2 C_0(y, z) \right).$$

By the Proposition 8.1.2 the solubility of this reduction is $p/(p+1)$, therefore the overall solubility in the two conjugate lines case is $\frac{1}{p+1}$.

**Double line case.**

Moving the double line to $y = 0$, the new $C_4(Y, Z)$ will still have no roots over $\mathbb{F}_p$, in particular the coefficients $a_{0,4,0}$ and $a_{0,0,4}$ of $T$ will still have valuations equal to 1. Therefore, after the substitution $T \to T(X, pY, Z)/p$, the reduction is $\overline{T} = z^4 + axz^3 + bx^2z^2 + cx^3z + dx^4$, with $a, b, c$ and $d$ in $\mathbb{F}_p$. Let us analyse the possible factorisations of the monic quartic:

- it has at least one simple root on $\mathbb{F}_p$, which has not $x$-coordinate equal to 0 since the presence of the term $z^4$, therefore we have solubility. This happens with probability equal to $\frac{5p^3-2p^2-p-2}{8p^3}$;
- no roots defined over $\mathbb{F}_p$, therefore we have no solubility. This happens with probability equal to $\frac{3p^3-2p^2+p-2}{8p^3}$;
- a quadruple root over $\mathbb{F}_p$. This happens with probability equal to $\frac{1}{p^3}$:
- one double root on $\mathbb{F}_p$. This happens with probability equal to $\frac{p-1}{2p^2}$;
- two double roots on $\mathbb{F}_p$. This happens with probability equal to $\frac{p-1}{2p^3}$.

For the last three cases we need further computations. We now deal with the double root one. We assume, after a change of variable, to have an equation of the form $z^2(ax^2 + bxz + z^2)$, and we check the probability that the points on $z^2 = 0$ lift, so $p|Z$. Of course the solubility is independent of the choice of the double line. Moreover, since the valuation of the coefficient of $z^4$ is zero we cannot have $x^2 = 0$ as a factor. By Proposition 8.1.1, the case with just one double root has solubility $1/2$. Therefore, when there are two double roots the probability is $1 - (1 - 1/2)^2 = 3/4$ by independence.

Let us consider the quadruple root case, without loss of generality we assume the reduction to be $z^4 = 0$.

After the substitution $T(X, Y, pZ)/p$ the reduction $\overline{T}$ is $x^2(y^2 + axy + by^2)$. The possible configurations are:

- two lines over $\mathbb{F}_p$, which implies at least a point to lift. This happens with probability $(p-1)/2p$;
- two conjugate lines $\mathbb{F}_p$, which means no point since the only singular point has $x$-coordinate equal to 0. This happens with probability $(p-1)/2p$;
- a double root, which we move to $y^2 = 0$. It happens with probability $1/p$.

Only in the latter case do we need further computation to obtain the solubility. After the substitution $T(X, pY, Z)/p$ the reduction is $x^3(az + bx)$. If $a \neq 0$ (which happens with probability equal to $(p-1)/p$) we have solubility, otherwise we continue if they both have valuation greater than 0, which happens with probability $1/p^2$. The remaining cases are discarded by primitivity. Then substituting $Y$ with $pY$ and dividing by $p$ we get the following triangle of valuations.

$$\begin{array}{lllllll} Z^4 & = 1 & & & & & \\ & \geq 1 & \geq 2 & & & & \\ & \geq 0 & \geq 1 & \geq 3 & & & \\ & \geq 0 & \geq 0 & \geq 2 & \geq 4 & & \\ X^4 & \geq 0 & \geq 0 & = 0 & \geq 3 & = 5 & Y^4 \end{array}$$

Table 8.1: Quartic with solubility $\tau$

Let $\tau$ be the probability of solubility of this reduction. Recall that a side condition is that we cannot lift points on the line $x = 0$. Here we want to achieve a recursive formula, where we can express $\tau$ in terms of itself. The process is basically the same as we have just seen apart from the fact that, due to the side condition on the coefficient of $X^2Y^2$, the probabilities of each possible configuration are a bit different. Let us describe in detail what is happening.

The equation has the form $x^2\gamma(x, y, z)$, where $\gamma$ is monic in $y^2$. Therefore, the ternary conic $\gamma$ can have one of the following factorisations:

- a line squared $(y + ax + bz)^2$, with probability $\frac{1}{p^3}$;
- two conjugate lines whose intersection is not on the line $x = 0$. This happens with probability $\frac{p-1}{2p^2}$;
- two distinct $\mathbb{F}_p$-rational lines, in this case we have solubility 1. This happens with probability $\frac{p^2-1}{2p^3}$;
- a smooth conic, where we have solubility 1. This happens with probability $\frac{p-1}{p}$.

The only cases where we should continue are the first two. When $\gamma$ is a product of conjugate lines we have already computed its solubility in Proposition 8.1.2: $\frac{1}{p+1}$. Instead when $\gamma$ is a line squared, we change the coordinates moving the double line to $y=0$. Notice that, by the side condition on $C_4(Y,Z)$ not having $\mathbb{F}_p$ roots, the valuation of the coefficient of $Z^4$ is not affected. After the usual substitution $T \to T(X,pY,Z)/p$ we have a monic quartic in $z$. The computation is basically the same as we have seen above, in particular, when the quartic has a quadruple root, we end up in a reduction really similar to the one that has solubility $\tau$:

$$\begin{array}{cccccc} Z^4 & = 1 & & & & \\ & \geq 1 & \geq 3 & & & \\ & \geq 0 & \geq 1 & \geq 4 & & \\ & \geq 0 & \geq 0 & \geq 2 & \geq 7 & \\ X^4 & \geq 0 & \geq 0 & = 0 & \geq 5 & \geq 9 \quad Y^4 \end{array}$$

Since, during the procedure, we are interested just in the coefficients of the terms in the set $\{X^2Y^2, X^3Y, X^2YZ, X^4, X^3Z, X^2Z^2, XZ^3, Z^4\}$ and they have the same valuations as in the triangle (8.1), then the solubility of this reduction is still $\tau$. Therefore, we obtain a recursive formula involving the probability of solubility $\tau$:

$$\begin{aligned}\tau =& \frac{p-1}{p} + \frac{p^2-1}{2p^3} + \frac{p-1}{2p^2(p+1)} \\ &+ \frac{1}{p^3}\left(\frac{5p^3-2p^2-p-2}{8p^3} + \frac{p-1}{4p^2} + \frac{3(p-1)}{8p^3} + \frac{1}{p^3}\Big(\frac{p-1}{2p} + \frac{1}{p}\Big(\frac{p-1}{p} + \frac{1}{p^2}\tau\Big)\Big)\right),\end{aligned}$$

We can now compute it explicitly:

$$\tau = \frac{p\left(8p^8+12p^7+12p^6+9p^5+10p^4+10p^3+9p^2+12p+8\right)}{8(p+1)\left(p^2+p+1\right)\left(p^6+p^3+1\right)}. \tag{8.1}$$

**Overall probability of solubility**

Weighting the solubility formulas computed above we obtain the overall probability of solubility

$$\begin{aligned}&\frac{p-1}{p^6-1}\left[\frac{p^4+2p^3+2p^2+p}{2} + p^5 - p^2 + \frac{p^4-p^3}{2(p+1)}\right. \\ &\left. + (p^2+p)\left(\frac{5p^3-2p^2-p-2}{8p^3} + \frac{p-1}{4p^2} + \frac{3(p-1)}{8p^3} + \frac{1}{p^3}\left(\frac{p-1}{2p} + \frac{1}{p}\Big(\frac{p-1}{p} + \frac{1}{p^2}\tau\Big)\right)\right)\right].\end{aligned}$$

□

## 8.2 Absolutely irreducible quartics

In the study of the solubility of the cubics that has been done in [BCF15a] the irreducible cases were not a concern: indeed a cubic curve has always a smooth point by the Hasse-Weil bound. This is not the case when the degree of the curve is 4. By the work [HLT05] by Howe, Lauter and Top we have that a smooth quartic over $\mathbb{F}_p$ has at least one rational point if $p > 29$. This rational point can be then lifted by Hensel's Lemma giving solubility. For the small primes it would be possible to investigate how many curves do have a rational point by counting. If the reduction is a singular quartic the bound on the characteristic of the base field is lower. Indeed, is possible we can work out sharper bounds for each possible irreducible reduction. The main result we will use is a bound on the number of rational points of an irreducible curve over a finite field. In our case of a quartic $\overline{T}$ defined over $\mathbb{F}_p$ we have

$$|\#\overline{T}(\mathbb{F}_p) - (p+1)| \leq 2\tilde{g}\sqrt{p} + \delta,$$

where $\tilde{g}$ is the geometrical genus of $\overline{T}$ and $\delta$ is the sum of the $\delta$-invariants of each point of $\overline{T}$, see [AP95] and [Stö93]. We point out that there are even sharper bounds, studied by Zúñiga Galindo in [ZG98], but our classification and counts of the singular curves is just in function of the $\delta$ invariant.

Let $s$ be the cardinality of the singular rational points on $\overline{T}$ then we have

$$\#\overline{T}_0(\mathbb{F}_p) \geq p + 1 - 2\tilde{g}\sqrt{p} - \delta - s, \tag{8.2}$$

where $\overline{T}_0$ is the set of smooth points of $\overline{T}$. For each possible irreducible reduction we want to determine the lower bound for $p$ such that the right-hand side of the equation (8.2) is strictly greater than 0 in order to guarantee smooth points on the reduction and hence solubility. We recall that we can have either just double points or at most one singular point of multiplicity three. In the latter case we have always solubility if $p \geq 3$, as described in Section (5.4.2). In the following table we describe the lower bounds for the remaining cases where, by the notation $[a, b, c]$ we mean a quartic that has $a$ singularities defined over $\mathbb{F}_p$, $b$ on $\mathbb{F}_{p^2}$ but not on $\mathbb{F}_p$ and $c$ on $\mathbb{F}_{p^3}$ but not on $\mathbb{F}_p$.

In any case, for $p$ greater than *or equal to* the bound, we do have a smooth point over the reduction and hence solubility. As expected the bound for singular curves is lower than the one for smooth curves.

| # Singularities | $\tilde{g}$ | $\delta$ | $s$ | Bound |
|---|---|---|---|---|
| $[1,0,0]$ | 2 | 1 | 1 | 19 |
| $[2,0,0]$ | 1 | 2 | 2 | 11 |
| $[0,2,0]$ | 1 | 2 | 0 | 7 |
| $[3,0,0]$ | 0 | 3 | 3 | 7 |
| $[1,2,0]$ | 0 | 3 | 1 | 5 |
| $[0,0,3]$ | 0 | 3 | 0 | 3 |

## 8.3 Conjugate conics

We have already considered the conjugate conics in the previous chapter, indeed they may intersect in different ways. We describe the different reductions by the set of $\mathbb{F}_p$-rational intersection points. The cases left are:

- one point with intersection multiplicity 2;
- two points with intersection multiplicity 2;
- one point with intersection multiplicity 2 and two points with intersection multiplicity 1;
- one point with intersection multiplicity 3 and one point with intersection multiplicity 1;
- one point with intersection multiplicity 4.

Let us study the probability of solubility case by case. The intersection multiplicity is characterized by the equation as described in 5.2.

### 8.3.1 One point with intersection multiplicity 2

We consider the product of two conjugate conics with just one $\mathbb{F}_p$-rational point of intersection, whose multiplicity of intersection is 2. The result, since the procedure involves the solubility absolutely irreducible quartics, describes the solubility for primes greater or equal than 19. We move the singular point to $P = [0 : 0 : 1]$; since the intersection multiplicity is at least 2 in $P$, the tangent lines at $P$ to the two conics coincide, we move them to $x = 0$. We can write this reduction as

$$\overline{T} = (Q(x, y) + xz)(\sigma(Q(x, y)) + xz),$$

where $Q(x, y)$ is a binary quadratic over $\mathbb{F}_{p^2}$ but not on $\mathbb{F}_p$, in order to have a product of irreducible conics the coefficient of $y^2$ in $Q$ should be not null. Moreover, since we want

$x \nmid Q - \sigma(Q)$ (this condition is equivalent to have multiplicity of intersection equal to 2) the coefficient $\alpha$ of $y^2$ has to be in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$. We refer to the probability of lifting the point $[0:0:1]$ as $\tau$.

The first necessary condition for lifting $P$ are the divisibility of $X$ and $Y$ coordinates by $p$. Then we can divide all the coefficients by $p$, the new reduction will be just $\overline{T} = az^4$. This reduction is not soluble by primitivity unless the coefficient $a$ of $z^4$ is zero, which happens with probability $1/p$. In this case we can divide further by $p$ ending up with the reduction

$$\overline{T} = z^2(az^2 + bxz + x^2 + cyz) = z^2\gamma.$$

Notice that the coefficient of $x^2z^2$ is equal to one since it is the same coefficient of the original reduction (since we multiplied it by $p^2$ and divided it by $p^2$). The coefficients $a$, $b$ and $c$ are uniformly and independently distributed on $\mathbb{F}_p$. If the conic defined by $\gamma = 0$ is smooth we are done, since it has at least one smooth point with $z$-coordinate different from 0. Looking at the determinant of the matrix associated to $\gamma$, the conic is irreducible if and only if $c \neq 0$, this happens with probability $(p-1)/p$. If we focus on the singular cases (they happen with probability $1/p$) we already know that on the line $z = 0$ there is a double point, it can be the intersection of two distinct lines defined over $\mathbb{F}_p$ (this case happens with probability $\frac{p-1}{2p}$, and we have solubility), or the intersection of two conjugate lines over $\mathbb{F}_{p^2}$ (this case happens with probability $\frac{p-1}{2p}$, and we have insolubility because the only $\mathbb{F}_p$ point has $z$-coordinate null and so it is not liftable by primitivity) or we can have a double line with probability $1/p$ which we move to $x = 0$.

A necessary condition now for liftability is that $p$ divides the $x$-coordinate of the solution, making the substitution and dividing by $p$ we end up with the following reduction

$$\overline{T} = z^2(az^2 + cyz + dy^2),$$

where $a$, $c$ and $d$ are uniformly and independently distributed on $\mathbb{F}_p$. If $d$ is non-zero (with probability $(p-1)/p$) then we have probability of solubility $1/2$ by Proposition 8.1.1. If $d = 0$ (with probability $1/p$) the reduction is $z^3(az + cy)$ and, if $c \neq 0$ which happens with probability $(p-1)/p$, we have a line which contains smooth points, which implies solubility. Otherwise, if $c = 0 = d$ (with probability $1/p^2$) the reduction is just $z^4a = 0$ where, by primitivity, we have potential solubility if $a = 0$ (with probability $1/p$).

The null quartic is the only case where we need to investigate further. After

division by $p$ these are the valuations of all the coefficients of the quartic

$$\begin{array}{cccccc} Z^4 & \geq 0 & & & & \\ & \geq 0 & \geq 0 & & & \\ & = 0 & \geq 0 & \geq 0 & & \\ & \geq 2 & \geq 1 & \geq 0 & \geq 0 & \\ X^4 & \geq 4 & \geq 3 & \geq 2 & \geq 1 & = 0 \quad Y^4 \end{array}$$

In particular, looking at the reduction $\overline{T}$ the coefficient of $xy^2z$ is the trace of the element $\alpha$ cited at the beginning, the one of $y^4$ is norm of $\alpha$ and the one of $x^2z^2$ is 1.

About this family of quartics we know that they have a singular point in $[1:0:0]$ with double tangent $z=0$. By primitivity we cannot lift this point. By interpolation on small primes we have the counts of the possible reduction of these quartics (in total there are $p^6$ of them):

- $p^6 - p^4$ are irreducible, therefore if the cardinality of the base field is greater or equal than 19, by Section 8.2, we have solubility 1.
- $p^4$ are products of conjugate conics, in particular the $\mathbb{F}_p$-rational intersection points are:
  - (i) One point with intersection multiplicity 2 in $(p^4-p^3)/2$ cases;
  - (ii) Two points with intersection multiplicity 2 in $p^3$ cases;
  - (iii) One point with intersection multiplicity 2 and two points with multiplicity of intersection 1 in $(p^4-p^3)/2$ cases.

Recalling that we cannot lift the point $Q=[1:0:0]$ the solubility of the undetermined cases above are as follows:

(i) The only singular point is $Q$, since we cannot lift any point;

(ii) This case has solubility $\tau$, since we can just lift the second point of interesection;

(iii) This case has solubility $\frac{2p+1}{p^2+2p+1}$, which is the solubility when we have two points with multiplicity 1.

Wrapping up we find

$$\tau = \frac{1}{p}\Big(\frac{p-1}{p}+\frac{1}{p}\Big(\frac{p-1}{2p}+\frac{1}{p}\Big(\frac{p-1}{2p}+\frac{1}{p}\Big(\frac{p-1}{p}+\frac{1}{p^2}\Big(\frac{1}{p^6}\Big(p^6-p^4+p^3\tau+\frac{p^4-p^3}{2}\frac{2p+1}{p^2+2p+1}\Big)\Big)\Big)\Big)\Big)\Big),$$

which give us the probability of solubility

$$\frac{2p^9+5p^8+5p^7+5p^6+5p^5+4p^4+6p^3+6p^2+4p+1}{2(p+1)^2\left(p^8+p^7+p^6+p^5+p^4+p^3+p^2+p+1\right)}.$$

### 8.3.2 Two points, both with intersection multiplicity 2

Here we study the case when the reduction $\overline{T}$ is a product of two conjugate conics intersecting in two points, both with intersection multiplicity 2. The result, since the procedure involves the solubility of absolutely irreducible quartics, describes the solubility for primes greater or equal than 19. We move the two intersection points to $[0:0:1]$ and $[1:0:0]$. Notice that the two tangent lines at the singular points are defined over $\mathbb{F}_p$ and distinct. Indeed, they are defined over $\mathbb{F}_p$ by the intersection multiplicity and they cannot be equal; otherwise having the same tangent would imply an intersection of order 4 between the line and conic, which would lead to a reducible conic by Bézout's Theorem. Therefore, we can move their $\mathbb{F}_p$-rational intersection point to $[0:1:0]$. We then have the following model, which factors over $\mathbb{F}_{p^2}$ as

$$\overline{T} = (\alpha y^2 + xz)(\sigma(\alpha)y^2 + xz),$$

where $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ and $\sigma$ is the Frobenius endomorphism.

A necessary condition is $p|Y$. After the substitution, the reduction is a product of two lines where we cannot lift the quadruple point, since it has both $x$ and $z$ coordinates congruent to 0 mod $p$ which, by primitivity, is a contradiction. Then we can either lift a point on $x=0$ or one on $z=0$, this corresponds to lifting one of the double points we had at the beginning. Without loss of generality we say $p|X$ and therefore, what we are about to compute, is the probability $\tau$ of lifting the point $[0:0:1]$.

This probability $\tau$ is not affected by the singularity of the reduction at the other point $[1:0:0]$, indeed going through the procedure we would repeat the same steps described in 8.3.1. In particular, all the conditions are about the coefficients of the monomials in the set $\{Z^4, XZ^3, YZ^3, XYZ^2, Y^2Z^2, Y^3Z\}$. Whereas, if we decide to lift the point $[1:0:0]$ assuming $p|Z$ we would deal with a disjoint set of coefficients: they would be the ones correspondent to the monomials in $\{X^4, X^3Y, X^3Z, X^2YZ, X^2Y^2, X^3Y\}$. Therefore the probabilities of lifting each of the two singular points are independent, and equal to the one described in section 8.3.1 and denoted there by $\tau$. So, the overall probability of liftability of this case is given by $1-(1-\tau^2)$. The numerator of this

probability of solubility is:

$$8p^{19} + 40p^{18} + 92p^{17} + 147p^{16} + 202p^{15} + 253p^{14} + 308p^{13} + 373p^{12} + 426p^{11} + 451p^{10} + 436p^9 + 390p^8 + 338p^7 + 282p^6 + 226p^5 + 172p^4 + 116p^3 + 60p^2 + 20p + 3$$

and its denominator is

$$4p^{20} + 24p^{19} + 68p^{18} + 128p^{17} + 192p^{16} + 256p^{15} + 320p^{14} + 384p^{13} + 448p^{12} + 504p^{11} + 528p^{10} + 504p^9 + 448p^8 + 384p^7 + 320p^6 + 256p^5 + 192p^4 + 128p^3 + 68p^2 + 24p + 4.$$

### 8.3.3 Three points, with intersection multiplicities 2, 1 and 1

Let $\overline{T} = \gamma\sigma(\gamma)$ be the reduction of $T$, where $\gamma$ is an irreducible conic defined over $\mathbb{F}_{p^2}$ but not on $\mathbb{F}_p$. When, like in this case, the reduction contains more than one $\mathbb{F}_p$-rational singular point, the key step is computing the probability of solubility is to understand how the liftability of each point is correlated with that of the others. In this case we prove that the three singular points can be lifted independently and therefore we can compute the total solubility using the formula for the case with just one point of intersection multiplicity equal to 2 and the one with two points of multiplicity the intersection equal to 1. The result, since the procedure involves the solubility of absolutely irreducible quartics, describes the solubility for primes greater or equal than 19.

We make a change of coordinates that sends the point $P$ with intersection multiplicity 2 to $[0:0:1]$ and the other two singular points $R$ and $S$ to $[1:0:0]$ and $[1:1:1]$. Moreover, we move the $\mathbb{F}_p$-rational double tangent line at $P$ to $x = 0$ (notice that this line does not contain other singular points apart from $P$). Therefore, the equation of $\gamma$ is

$$\gamma = \alpha y^2 - (\alpha + 1)xy + xz,$$

where $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$.

Then, during the procedure described in Section 8.3.1, all the conditions are about the coefficients of the monomials in the set $\{Z^4, XZ^3, YZ^3, XYZ^2, Y^2Z^2, Y^3Z\}$, so the liftability of the point $P$ depends just on those coefficients. Whereas the liftability of $R$, as described in (7.3.2), depends just on the coefficient $a_{4,0,0}$. Moreover, with the same ideas described in (7.4.1), we can swap by a change of coordinates $R$ and $S$, in order to determine the liftability of $S$ in terms of the coefficient $a_{2,1,1}$. In this way the probabilities $\tau_P$, $\tau_R$ and $\tau_S$ of lifting respectively $P$, $R$ and $S$ are pairwise independent. We already know $\tau_R = \tau_S = \frac{1}{p+1}$, whereas $\tau_R$ has been computed in Section 8.3.1, therefore the

overall probability of solubility in this case is

$$\frac{6p^{11}+19p^{10}+27p^9+29p^8+29p^7+28p^6+30p^5+30p^4+28p^3+21p^2+10p+2}{2(p+1)^4\left(p^2+p+1\right)\left(p^6+p^3+1\right)}.$$

### 8.3.4 Two points, with intersection multiplicities 3 and 1

In this section we study the case of a product of two conjugate conics $\gamma$ and $\sigma(\gamma)$, that intersect in two $\mathbb{F}_p$-rational points, with intersection multiplicities 1 and 3. For this case we are not able to compute an exact formula but just a close estimation. The result, since the procedure involves the solubility of absolutely irreducible quartics, describes the solubility for primes greater or equal than 19. We move the first point to $[1:0:0]$, the second to $[0:1:0]$. Note that the tangent at the point $P=[0:1:0]$ and the quartic intersect just in the point $P$, since the intersection multiplicity at $P$ is 4. Then, the other singular point $[1:0:0]$, is not contained in the tangent at $P$. We fix this tangent line as $x=0$, therefore we would have $\gamma = xy+\alpha xz+cz^2$, where $\alpha \in \mathbb{F}_{p^2}\setminus\mathbb{F}_p$ and $c\in\mathbb{F}_p\setminus\{0\}$. So the reduction of $T$ would be

$$\overline{T} = x^2y^2+N(\alpha)x^2z^2+c^2z^4+Tr(\alpha)x^2yz+2cxyz^2+cTr(\alpha)xz^3.$$

It follows that all coefficients of the terms above have valuations exactly zero but the ones of $x^2yz$ and $xz^3$, they may be both either equal to zero or strictly greater than zero. We already know, by Proposition 7.3.2, that the probability of lifting the point $[1:0:0]$ depends just on the coefficient $a_{4,0,0}$ and it is equal to $1/(p+1)$. Let us compute the probability $\tau$ of lifting the point $P$. A first necessary condition is $p|X$ and $p|Z$, after substituting and dividing by $p$ we get as reduction $\overline{T}=ay^4$.

Then, the reduction steps are basically identical to the ones in section 8.3.1 until the really last one, where the reduction is a bit different. Indeed, we would end up in the following triangle of valuations:

$$\begin{array}{llllll}
Z^4 & =0 & & & & \\
 & \geq 1 & \geq 0 & & & \\
 & =2 & =0 & \geq 0 & & \\
 & \geq 4 & \geq 1 & \geq 0 & \geq 0 & \\
X^4 & \geq 5 & \geq 3 & =0 & \geq 0 & \geq 0 \quad Y^4
\end{array}$$

Let $\eta$ be the probability of solubility of this reduction, with the side condition that $p\nmid Y$.

Therefore the probability $\tau$, of lifting the initial singular point $P$, would be

$$\tau = \frac{1}{p}\left(\frac{p-1}{p} + \frac{1}{p}\left(\frac{p-1}{2p} + \frac{1}{p}\left(\frac{p-1}{2p} + \frac{1}{p}\left(\frac{p-1}{p} + \frac{1}{p^2}\eta\right)\right)\right)\right).$$

Moreover, during all this procedure, the coefficient $a_{4,0,0}$ has not been involved in any condition, therefore this probability $\tau$ is independent of the solubility of the other singular point. Indeed, by Proposition 7.3.2 and the following remark, we have that the solubility of the point $[1:0:0]$ is $1/(p+1)$ and depends just on the coefficient $a_{4,0,0}$.

It remains just to compute $\eta$. At this step, the terms which have valuation exactly equal to zero are $x^2y^2 + c^2z^4 + 2cxyz^2 = (xy + cz^2)^2$, where $c$ is the element of $\mathbb{F}_p$ stated at the beginning of this section.

About this family of quartics we know that they have a singular point in $[1:0:0]$ with double tangent $y = 0$. By primitivity we cannot lift this point. By interpolation on the small primes we have the counts of the possible reduction of these quartics, in total there are $p^6$ different quartics.

(i) $p^6 - p^4$ are irreducible, therefore if the cardinality of the base field is greater or equal than 19 we have solubility as described in Section 8.2.

(ii) $p^2(p^2-1)/2$ are conjugate conics, They are divided in:

  (a) $p^2(p-1)/2$ with just one point with intersection multiplicity equal to 4, that coincides with the point we cannot lift, therefore we have insolubility.

  (b) $p^2(p^2-p)/2$ which have 2 points with intersection multiplicity equal to 3 and 1. We cannot lift the one with multiplicity 3 but the other one is out of the line $y = 0$ so the solubility of this case is equal to the solubility of the product of conjugate conics having just one point with multiplicity 1. Then, in this case the solubility is $1/(p+1)$.

(iii) $p^2(p^2+1)/2$ are a product of two irreducible conics. They split in:

  (a) $p^2$ irreducible conics squared, from those we can lift any point but $[1:0:0]$.

  (b) $p^2(p^2-1)/2$ distinct irreducible conics, which for $p > 3$ have at least one smooth point, therefore we have solubility.

It remains to deal just with the case iii-a. Unfortunately we do not have a closed formula for the solubility of a conic squared, therefore we cannot deduce a closed formula for this

case as well. Since the solubility of the conic squared is trivially between 0 and 1, we can give an upper bound and a lower bound on $\eta$:

$$p^6 - p^4 + \frac{p^2(p^2-p)}{2(p+1)} + p^2(p^2-1)/2 \leq p^6\eta \leq p^6 - p^4 + \frac{p^2(p^2-p)}{2(p+1)} + p^2(p^2-1)/2 + p^2,$$

therefore the order we have $\eta \sim 1 - \frac{1}{p^4}$. The inequalities imply other inequalities on $\tau$ and, by the independence with the solubility of the point $[1:0:0]$ we can compute the total solubility as

$$1 - (1-\tau)\left(1 - \frac{1}{p+1}\right).$$

Therefore, we can compute a lower bound for this solubility as

$$\frac{4p^{10} + 3p^9 - p^8 + p^7 - p^6 + 2p^4 - p^3 - 2p - 1}{2p^9(p+1)^2}$$

and an upper bound

$$\frac{4p^{10} + 3p^9 - p^8 + p^7 - p^6 + 2p^4 - p^3 + 1}{2p^9(p+1)^2}.$$

Notice that the difference between upper and lower bound is strictly smaller than $p^{-10}$.

### 8.3.5 One point with intersection multiplicity 4

Here we study the case of a product of conjugate conics $\gamma\sigma(\gamma)$ whose intersection consists of a $\mathbb{F}_p$-rational point with multiplicity 4. For this case we are not able to compute an exact formula but just a close estimation. The result, since the procedure involves the solubility of absolutely irreducible quartics, describes the solubility for primes greater or equal than 19. We move the point to $[1:0:0]$ and its tangent line to $y=0$, moreover we complete the square in order to have no term in $yz$. Therefore, we would have $\gamma = xy + \alpha y^2 + cz^2$, where $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ and $c \in \mathbb{F}_p \setminus \{0\}$. So the reduction of $T$ would be

$$x^2y^2 + N(\alpha)y^4 + c^2z^4 + 2cxyz^2 + Tr(\alpha)(xy^3 + cy^2z^2),$$

from this it follows that all coefficients of the terms outside the brackets have valuations exactly zero and the ones inside have either all valuations equal to zero or all strictly greater than zero up to the trace of $\alpha$. Let $\tau$ the probability of lifting the point $[1:0:0]$ to a point in $\mathbb{P}^2(\mathbb{Q}_p)$. We start with the usual reduction steps, repeating basically the procedure described in 8.3.1 until the really last one, where the reduction is a bit different.

Indeed, the triangle of valuations is

$$\begin{array}{cccccc} Z^4 & = 0 & & & & \\ & \geq 0 & \geq 2 & & & \\ & \geq 0 & = 0 & \geq 2 & & \\ & \geq 0 & \geq 0 & \geq 2 & \geq 4 & \\ X^4 & \geq 0 & \geq 0 & = 0 & \geq 2 & = 4 \quad Y^4 \end{array}$$

and, referring to the solubility of this reduction as $\eta$, we have

$$\tau = \frac{1}{p}\left(\frac{p-1}{p} + \frac{1}{p}\left(\frac{p-1}{2p} + \frac{1}{p}\left(\frac{p-1}{2p} + \frac{1}{p}\left(\frac{p-1}{p} + \frac{1}{p^2}\eta\right)\right)\right)\right).$$

About this family of quartics we know that they have a singular point in $[0:1:0]$ with double tangent $x = 0$. By primitivity we cannot lift any point on $x = 0$ and hence this singular point. By interpolation on the small primes we have the counts of the possible reductions (in total there are $p^6$ of them):

(i) $p^6 - p^4$ are irreducible, therefore if the cardinality of the base field is greater or equal than 19 we have solubility by 8.2.

(ii) $p^2(p^2-1)/2$ are conjugate conics. They are divided in:

  (a) $p^2(p-1)/2$ which have just one point with intersection multiplicity equal to 4, but we cannot lift it, therefore we have insolubility.

  (b) $p^2(p^2-p)/2$ which have 2 $\mathbb{F}_p$-rational points with intersection multiplicities equal to 3 and 1. We cannot lift the one with multiplicity 3 but the other one is not on the line $x = 0$ so the solubility of this case is equal to the solubility of the conjugate conics having just one point with multiplicity 1, i.e. $1/(p+1)$.

(iii) $p^2(p^2+1)/2$ are a product of two irreducible conics. They split in:

  (a) $p^2$ irreducible conics squared, from those we can lift any point but $[1:0:0]$.

  (b) $p^2(p^2-1)/2$ distinct irreducible conics, which for $p > 3$ have at least one smooth point, therefore we have solubility.

It remains to deal just with the case iii-a. Unfortunately we do not have a closed formula for the solubility of a conic squared, therefore we cannot deduce a closed formula

for this case as well. Since the solubility of the conic squared is trivially between 0 and 1, we can give an upper bound and a lower bound on $\eta$:

$$p^6 - p^4 + \frac{p^2(p^2-p)}{2(p+1)} + p^2(p^2-1)/2 \leq p^6\eta \leq p^6 - p^4 + \frac{p^2(p^2-p)}{2(p+1)} + p^2(p^2-1)/2 + p^2,$$

therefore the order we have $\eta \sim 1 - \frac{1}{p^4}$. The inequalities imply other inequalities on $\tau$ which are

$$\frac{2p^{10}+p^9-p^8+p^7-p^6+2p^4-p^3-2p-1}{2p^{10}(p+1)} \leq \tau \leq \frac{2p^{10}+p^9-p^8+p^7-p^6+2p^4-p^3+1}{2p^{10}(p+1)}.$$

Notice that $\tau \sim \frac{1}{p+1}$ and that the error on the probability of this solubility is bounded by $p^{-10}$.

## 8.4 Reductions with just one $\mathbb{F}_p$-rational quadruple point

If the reduction of the quartic $T$ has just one $\mathbb{F}_p$-rational point, that is a quadruple point, assuming it in $[0:1:0]$ we have $\overline{T} = C_4(x,z)$, where $C_4$ is homogeneous of degree 4 with no roots over $\mathbb{F}_p$. The three possible factorisations of $C_4$ correspond to three different reductions: 4 conjugate lines over $\mathbb{F}_{p^4}$, 2 distinct pairs of conjugate lines over $\mathbb{F}_{p^2}$, two conjugate lines over $\mathbb{F}_{p^2}$ squared. The procedure to compute the solubility of these cases is really similar due to the similar geometrical structure (basically $\overline{T}=0$ is 4 concurrent lines) so we will describe their probability of solubility together.

**Proposition 8.4.1.** *Let $T$ be a ternary quartic over $\mathbb{Z}_p$ whose reduction has just one $\mathbb{F}_p$-rational point, that is singular of multiplicity 4. Then, the probability of solubility of $T$ is contained in the set*

$$\frac{8p^{14}-8p^{12}+16p^{11}-4p^{10}-4p^9+9p^8+4p^7-12p^6+4p^4-8p^3-p^2+4p-8}{8p^9\left(p^6+p^3+1\right)} + \left[0, \frac{1}{p^{10}}\right].$$

*Proof.* The reduction over $\mathbb{P}^2(\mathbb{F}_p)$, assuming the singular point is $P=[0:1:0]$, has the following equation

$$\overline{T} = C_4(x,z),$$

where $C_4$ has no roots over $\mathbb{F}_p$. We then proceed with the usual substitution $T' = \frac{1}{p}T(pX,Y,pZ)$ and, renaming $T'$ with $T$, we get $\overline{T} = ay^4$. By primitivity, in order to have solubility, $a$ has to be zero, which happens with probability $1/p$. Then, dividing again by $p$, the reduction is $y^4 + y^3C_1(x,z)$. If $C_1(x,z) \neq 0$ we have solubility, since

we have a line times $y^3$; this happens with probability $(p^2-1)/p^2$. Otherwise, to have solubility, by primitivity, the reduction of $C_2$ has to be null, this happens with probability $1/p^3$. Dividing by $p$ again we have $y^2C_2(x,y,z)=0$. In the case $C_2$ is not the constant 0 this reduction is discussed in the Proposition 8.1.3, let $\tau$ be its solubility. If $C_2=0$, we divide $T$ by $p$ and get a generic quartic whose intersection with the line $y=0$ is $C_4=0$. Let $\theta$ the probability of solubility of this reduction. Then the overall solubility is

$$\frac{1}{p}\left(\frac{p^2-1}{p^2}+\frac{1}{p^3}\left(\frac{p^6-1}{p^6}\tau+\frac{\theta}{p^6}\right)\right).$$

In order to compute $\theta$, and therefore the overall probability of solubility, we would need to consider all the possible reductions that satisfy the side condition of intersection with the line $y=0$, compute combinatorially the number of such curves for each type and then weight the counts with the solubility of each specific reduction. This computation depends on how $C_4$ factors over $\mathbb{F}_{p^4}$, and at each possible factorisation corresponds a different initial reduction. Analysing the possible reduction types satisfying the different side conditions we have:

- If $C_4$ has 4 conjugate roots over $\mathbb{F}_{p^4}$, then the possible reduction types are: absolutely irreducible quartic, 4 conjugate lines over $\mathbb{F}_{p^4}$, two conjugate conics.
- If $C_4$ has 2 pairs of conjugate roots over $\mathbb{F}_{p^2}$, then the possible reduction types are: absolutely irreducible quartic, 2 pairs of conjugate lines over $\mathbb{F}_{p^2}$ either with or without the quadruple point, two conjugate conics.
- If $C_4$ has 2 double conjugate roots over $\mathbb{F}_{p^2}$, then the possible reduction types are: absolutely irreducible quartic, 4 conjugate lines over $\mathbb{F}_{p^4}$, two conjugate conics, two pairs of conjugate lines without quadruple point, a conic squared, two conjugate lines squared.

Moreover, each count regarding two conjugate conics should be done for any of the 8 possible configurations, since they have different solubilities and the proportion of them satisfying the side conditions vary with the configuration.

At the end of the process, in any case, we would obtain just an estimation of the value of the overall probability of solubility since for some of the reductions involved, we have no exact formula for their solubility. Already at this stage, saying that $\theta\in[0,1]$, describes the probability of solubility with an error of $p^{-10}$, which is rather negligible in comparison to the other estimations we made for other types of reduction. Saying that,

taking into account that most of the quartics satisfying the side condition are irreducible, we have that $\theta(p) \to 1$ for $p \to \infty$.

Plugging the value of $\tau$ in the formula we then obtain the result. □

## 8.5 Not-reduced reductions

In the list of not semistable reductions there are the non-reduced ones. The issues in studying such reductions consist in dealing with a number of singular points which depends on $p$. For instance a quadruple line, such $x^4 = 0$, has $p + 1$ singular points in $\mathbb{P}^2(\mathbb{F}_p)$ and the probability of lifting one of them may depend on the probability of lifting the others, therefore computing the overall liftability may be difficult. As shown in Lemma 6.2.1, there is a dependency between the probability of lifting the singular points over a line squared in $\mathbb{P}^2(\mathbb{Q}_p)$, indeed there are just 7 possible cardinalities for the set of points lifted even though a priori they may any of the value between 0 and $p + 1$.

It follows that there are correlations between the liftabilities of each point on the reduction and, in order to express a closed formula regarding the probability of solubility of each not-reduced reduction, we need to compute these correlations. Unfortunately, in some cases we are not able to compute all the dependencies, but we still furnish an estimate of the solubility overall.

### 8.5.1 Two conjugate lines times a double line, without point of multiplicity 4

**Proposition 8.5.1.** *Let $T$ be a ternary quartic over $\mathbb{Z}_p$ whose reduction is two conjugate lines times a double line, without point of multiplicity 4. Then, the probability of solubility of $T$ is*

$$\begin{aligned}&15p^{31} + 93p^{30} + 246p^{29} + 423p^{28} + 579p^{27} + 732p^{26} + 972p^{25} + 1284p^{24} + 1528p^{23}\\&+ 1632p^{22} + 1671p^{21} + 1695p^{20} + 1686p^{19} + 1629p^{18} + 1503p^{17} + 1224p^{16} + 948p^{15}\\&+ 740p^{14} + 612p^{13} + 456p^{12} + 288p^{11} + 60p^{10} - 84p^9 - 120p^8\\&- 120p^7 - 108p^6 - 120p^5 - 156p^4 - 156p^3 - 120p^2 - 60p - 12\end{aligned}$$

*divided by*

$$24p^9(p+1)^4\left(p^2+p+1\right)^2\left(p^6+p^3+1\right)\left(p^8-p^7+p^6+p^2-p+1\right),$$

*plus* $\varepsilon$*, where* $\varepsilon \in \left[0, \frac{1}{p^9(1+p)(1+p+p^2)(1-p+p^2+p^6-p^7+p^8)}\right]$.

*Proof.* Without loss of generality we assume the reduction of $T$ to be

$$\overline{T} = x^2(y+\alpha z)(y+\sigma(\alpha)z),$$

where $\sigma$ is the Frobenius of $\mathrm{Gal}(\mathbb{F}_{p^2}, \mathbb{F}_p)$ and $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. Here we have two types of singular points, the one at $[1:0:0]$, with two conjugate tangents, and the ones on $x=0$. For the former we have probability of solubility $\frac{1}{p+1}$, by Proposition 7.3.2, and the solubility is determined just by the coefficient of $X^4$ in $T$.

Let us discuss the singular points on the double line $x=0$; we refer to the solubility of the entire line, i.e the probability that at least one of the $p+1$ points lifts, as $\tau$. The first substitution is $T(pX,Y,Z)/p$, which gives us the new reduction $\overline{T} = C_4(y,z)$, with no condition on the binary quadric $C_4$. Looking at the possible factorisations on $\mathbb{F}_p$ of the binary quartics, recalling the results from Lemma 5.3.3, we have:

- Irreducible, therefore there are no point to lift by primitivity. This happens with probability equal to $\frac{3p^4-5p^3+3p^2-3p+2}{8p^4}$.
- It has at least one single root, in this case it lifts and we have solubility. This happens with probability equal to $\frac{5p^4+p^3-3p^2-p-2}{8p^4}$.
- Just one double root. This happens with probability equal to $\frac{p^3-p^2-p+1}{2p^4}$.
- Two double roots. This happens with probability equal to $\frac{p^2-1}{2p^4}$.
- A quadruple root. This happens with probability equal to $\frac{p^2-1}{p^5}$.
- The null quartic. This happens with probability equal to $\frac{1}{p^5}$.

The last 4 cases are undetermined. First we deal with the single double root case. Therefore, without loss of generality, we assume the equation of $\overline{T}$ to be of the form $y^2(z^2+ayz+by^2)$, with $a,b$ uniformly distributed in $\mathbb{F}_p$. Then, since $p|Y$, we make the substitution $T(X,pY,Z)/p$, getting as reduction $\overline{T} = z^2(x^2+a'xz+b'z^2)$, with $a',b'$ uniformly distributed in $\mathbb{F}_p$. The triangle of valuations in this case is the following:

$$\begin{array}{cccccccc}
Z^4 & \geq 0 & & & & & & \\
 & \geq 0 & \geq 1 & & & & & \\
 & = 0 & \geq 1 & = 1 & & & & \\
 & \geq 2 & \geq 1 & \geq 2 & \geq 2 & & & \\
X^4 & \geq 3 & \geq 3 & = 2 & \geq 3 & \geq 3 & Y^4 &
\end{array}$$

By Proposition 8.1.1 the solubility of this reduction is 1/2. Therefore, we have solubility 1/2 in the case of just one double root and $(1-(1-1/2)^2) = 3/4$ in the case with two double roots, since the probabilities of lifting each of the two points are independent.

In the case of a quadruple root, without loss of generality we assume the reduction to be $y^4 = 0$, which implies $p|Y$. Applying the substitution $T(X, pY, Z)/p$ we obtain the reduction $z^2(x^2 + axz + bz^2)$, with $a, b$ uniformly distributed in $\mathbb{F}_p$. Unfortunately here not all the hypothesis of the Proposition 8.1.1 are satisfied, therefore we need to make an ex-novo computation for this specific case.

By primitivity we have that $p \nmid z$, therefore we can lift only points on $x^2 + axz + bz^2 = 0$, let us describe its roots:

- Two conjugate roots, but this would imply $p|Z$, which is impossible by primitivity, so no solubility. This happens with probability $(p-1)/2p$.
- Two $\mathbb{F}_p$-roots, then we can lift them and conclude. This happens with probability $(p-1)/2p$.
- A double root. This happens with probability $1/p$.

The only undetermined case is the last one. Assuming the double line to be $x = 0$ we have, after the substitution $T(pX, Y, Z)/p$, that the reduction is $\overline{T} = z^3(az + by)$. If $a \neq 0$, which happens with probability equal to $\frac{p-1}{p}$, we have a linear factor and so liftability. Otherwise, by primitivity, it forces $b = 0$, which happens with probability $1/p^2$. Dividing by $p$ we get the following triangle of valuations for $T$:

$$\begin{array}{lllllll} Z^4 & \geq 0 & & & & & \\ & \geq 0 & \geq 0 & & & & \\ & = 0 & \geq 0 & \geq 0 & & & \\ & \geq 3 & \geq 1 & \geq 1 & \geq 1 & & \\ X^4 & \geq 5 & \geq 4 & = 2 & \geq 2 & = 1 & Y^4 \end{array}$$

The solubility of this reduction has been studied in the proof of the Proposition 8.1.3, and is the value described in the equation (8.1). We refer to this value as $\theta$.

The last remaining case is the null quartic. Then, after we divide by $p$, we have the following triangle of valuations:

$$\begin{array}{cccccc} Z^4 & \geq 0 & & & & \\ & \geq 0 & \geq 0 & & & \\ & = 0 & \geq 0 & \geq 0 & & \\ & \geq 2 & \geq 0 & \geq 0 & \geq 0 & \\ X^4 & \geq 3 & \geq 2 & = 0 & \geq 0 & \geq 0 \quad Y^4 \end{array}$$

This reduction has $[1:0:0]$ as singular point, with two conjugate tangent lines. We cannot lift this singular point by primitivity. We can investigate this reduction by interpolation on the small primes, which give us this distribution of the $p^9$ cases:

- $p^2$: line squared times two conjugate lines, where we cannot lift the intersection of the two conjugate lines, therefore its solubility is $\tau$.
- $p^2(p^2-1)/2$: two conjugate lines times two distinct lines, where we have solubility.
- $p^2(p^2-1)/2$: two pairs of conjugate lines, where the rational intersection points are distinct. We can lift just one of them with probability $1/(p+1)$.
- $p^4(p-1)$: conic times two conjugate lines, which has solubility 1.
- $p^4(p^2-1)$: two conjugate conics.
- $p^4(p^2-1)$: cubic times a line, where we have solubility.
- $p^9-2p^6-p^5+2p^4$: absolutely irreducible quartics, for $p \geq 19$ we have solubility by Proposition 8.2.

Between the $p^4(p^2-1)$ conjugate conics, we have:

- $\frac{1}{3}(p-1)^2p^3(p+1)$ with $m=1$, here we have insolubility.
- $p^2\left(p^2-1\right)$ with $m=1,3$, here we have bounds on the solubility of the point with intersection multiplicity equal to 3, which we denote $m_3$.
- $\frac{1}{2}(p-2)(p-1)p^2(p+1)^2$ with $m=1,1$, since we can lift just the second singular point we have solubility $1/(p+1)$.
- $2(p-1)p^3(p+1)$ with $m=1,1,2$, by the independence between the solubility of the three points we can compute the solubility using the formulas in Section 8.3.3. We therefore have solubility equal to $m_{12}=\frac{4p^{10}+11p^9+13p^8+13p^7+13p^6+12p^5+14p^4+14p^3+12p^2+7p+2}{2(p+1)^3\left(p^2+p+1\right)\left(p^6+p^3+1\right)}$.
- $\frac{1}{6}(p-1)p^3(p-7)(1+p)$ with $m=1,1,1,1$, so the solubility in this case is $(1-(1/(p+1))^3)=\frac{p^3+3p^2+3p}{(p+1)^3}$.

Therefore we have:

$$\begin{aligned}\tau =&\frac{3\left(p^2-1\right)}{8p^4}+\frac{p^3-p^2-p+1}{4p^4}+\frac{5p^4+p^3-3p^2-p-2}{8p^4}+\frac{\left(\frac{\frac{\theta}{p^2}+\frac{1}{p}}{p}+\frac{p-1}{2p}\right)\left(p^2-1\right)}{p^5}\\&+\frac{1}{p^{14}}\Bigg(p^2\tau+p^2(p-1)/2+p^4(p-1)+p^4(p^2-1)+p^9-2p^6-p^5+2p^4\\&+\frac{1}{2}(p-2)(p-1)p^2(p+1)+2(p-1)p^3(p+1)m_{12}\\&+\frac{1}{6}(p-1)p^3(p-7)(1+p)\frac{p^3+3p^2+3p}{(p+1)^3}+p^2\left(p^2-1\right)m_3\Bigg).\end{aligned}$$

In the above equation $m_{1,2}$ and $\theta$ are known, for $m_3$ we have an estimate with an error of $p^{-10}$. We can now estimate the value of $\tau$ by this recursive formula. Once we have that we can compute the overall solubility of this case, notice that in the computation of the solubility for the points on the line $x=0$ we have never considered the coefficient of $X^4$ of $T$, therefore the two probabilities of solubility computed are independent. Then the overall probability of solubility is $1-\frac{p}{p+1}(1-\tau)$ which we can estimate as

$$\begin{aligned}&15p^{31}+93p^{30}+246p^{29}+423p^{28}+579p^{27}+732p^{26}+972p^{25}+1284p^{24}+1528p^{23}\\&+1632p^{22}+1671p^{21}+1695p^{20}+1686p^{19}+1629p^{18}+1503p^{17}+1224p^{16}+948p^{15}\\&+740p^{14}+612p^{13}+456p^{12}+288p^{11}+60p^{10}-84p^9-120p^8\\&-120p^7-108p^6-120p^5-156p^4-156p^3-120p^2-60p-12\end{aligned}$$

divided by

$$24p^9(p+1)^4\left(p^2+p+1\right)^2\left(p^6+p^3+1\right)\left(p^8-p^7+p^6+p^2-p+1\right),$$

plus $\varepsilon$, where $\varepsilon\in\left[0,\frac{1}{p^9(1+p)(1+p+p^2)(1-p+p^2+p^6-p^7+p^8)}\right]$.

□

### 8.5.2 Double line and two conjugate lines with a quadruple point

Without loss of generality we have that the reduction is $\overline{T}=x^2(y+\alpha x)(y+\sigma(\alpha)x)$, with $\sigma$ the usual Frobenius and $\alpha\in\mathbb{F}_{p^2}\setminus\mathbb{F}_p$.

Here we have two different types of singular points: the quadruple one $[0:0:1]$ or the others on the line $x=0$, that are doubles. For the latter ones we have already

computed the solubility in the case of two double lines, indeed from (8.5) we have the probability of solubility of these points.

If we try to lift the quadruple point the first substitution is $T(pX, pY, Z)/p$, which leads us to the reduction $\overline{T} = az^4$. By primitivity $p \nmid Z$ so to continue we need $a = 0$, which happens with probability $\frac{1}{p}$.

Then, dividing by $p$, the reduction is $\overline{T} = z^3(ax + by + cz)$. If the linear factor is not $z$ we have solubility, this happens with probability $\frac{p^2-1}{p^2}$, otherwise we continue if the reduction is the null quartic, which happens with probability $\frac{1}{p^3}$.

Dividing by $p$ we get the following triangle of valuations:

$$\begin{array}{cccccc} Z^4 & \geq 0 & & & & \\ & \geq 0 & \geq 0 & & & \\ & \geq 0 & \geq 0 & \geq 0 & & \\ & \geq 1 & \geq 1 & \geq 1 & \geq 1 & \\ X^4 & = 1 & \geq 1 & = 1 & \geq 2 & \geq 2 \quad Y^4 \end{array}$$

Table 8.2:

Therefore, this reduction is $\overline{T} = z^2 C_2(x, y)$. As usual, according to the different possible factorisations of $C_2$ we have different probabilities of solubility. If $\overline{C_2}$ is not null, which happens with probability $\frac{1}{p^6}$, the conic $\overline{C_2}(x, y, z)$ can have one of the following factorisations:

- a line squared whose equation has a non-zero term in $y$, which happens with probability $\frac{p^2}{p^5+p^4+p^3+p^2+p+1}$;
- a line squared whose equation is of the form $x + az = 0$, which happens with probability $\frac{p}{p^5+p^4+p^3+p^2+p+1}$;
- two conjugate lines whose intersection is not on the line $z = 0$, which happens with probability $\frac{p^4-p^3}{2(p^5+p^4+p^3+p^2+p+1)}$;
- $z^2 = 0$, which happens with probability $\frac{1}{p^5+p^4+p^3+p^2+p+1}$. In this case, by primitivity, we have no solubility;
- two conjugate lines whose intersection is on the line $z = 0$, which happens with probability $\frac{p^3-p}{2(p^5+p^4+p^3+p^2+p+1)}$. In this case, by primitivity, we have no solubility;
- two dinstinct lines, which happens with probability $\frac{p^4+2p^3+2p^2+p}{2(p^5+p^4+p^3+p^2+p+1)}$. In this case there is at least one smooth point to lift;

- a smooth conic,which happens with probability $\frac{p^5-p^2}{p^5+p^4+p^3+p^2+p+1}$. Here again we have a smooth point to lift.

### Double line $ax + y + bz = 0$

In the first case we move the double line to $y = 0$ and proceed with the usual methods, with the substitution $T(X, pY, Z)/p$.

Before doing that is important to point out that this choice of the double line is actually without loss of generality. Indeed, in the case that the original double line is $ax + y + bz = 0$, with $a$ not null, we may change the coordinates in such a way the double line becomes $x = 0$ and make the substitution $T(pX, Y, Z)/p$. Since the triangle of valuations from Table 8.2 is not symmetric in $X$ and $Y$ it may look that this choice could affect the probability and therefore losing generality. Actually all the relevant valuation in the procedure turn up to be exactly the same, in particular the next step involves, after the substitution $T(pX, Y, Z)/p$, the binary quartic $C_4(y, z)$ instead of $C_4(x, z)$ (that would be the quartic object of study if we had moved the double line to $y = 0$). The latter is a monic quartic but the former does not look the same at the first glance. The valuation of the coefficient of $Y^4$ before of the change of the coordinates was greater or equal than 2, actually now it is equal to 1, which gives us a monic quartic for $C_4(y, z)$ as well. Indeed, by the change of coordinates that sends $X$ to $-aX + Y - bZ$, and fixes $Y$ and $Z$, we have that $a'_{0,4,0}$, the new coefficient of $Y^4$, is a linear combination of the previous coefficients of $C_4(X, Y)$, in particular three of them have valuations equal to 1 ($a_{4,0,0}$, $a_{3,1,0}$ and $a_{2,2,0}$) whilst the others have higher valuations. Therefore, considering the initial condition on the reduction, the first $p$-adic digit of $a'_{0,4,0}$ is

$$a'_{0,4,0}/p = \mathrm{N}(\alpha) + \mathrm{Tr}(\alpha) + 1 = (\alpha + 1)(\alpha^p + 1) \mod p.$$

The right-hand side is zero if $\alpha$ is either -1 or it is a primitive $2p$-th root of unity, the latter is not contained in $\mathbb{F}_{p^2}$ since to $2p \nmid (p^2-1)$, the order of the multiplicative group $\mathbb{F}^*_{p^2}$. Therefore, since $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ the equation is always non-zero and so $v(a'_{0,4,0}) = 1$.

Saying that we can really assume that without loss of generality the double line is $y = 0$. After the substitution $T(X, pY, Z)/p$ the reduction is the monic quartic $C_4(x, z)$, the solubility in this case has been already studied in the Proposition 8.1.3, in particular in the section *Double line case*, where we state with the equation (8.1) the solubility of

this case

$$\theta = \frac{p\left(8p^8 + 12p^7 + 12p^6 + 9p^5 + 10p^4 + 10p^3 + 9p^2 + 12p + 8\right)}{8(p+1)\left(p^2+p+1\right)\left(p^6+p^3+1\right)}.$$

### Double line $x + bz = 0$

If the double line is of the form $x + bz = 0$ we have a different scenario which justifies the choice of making two separate cases. Indeed, setting the double line to $x = 0$, after the substitution $T(pX, Y, Z)/p$ we have the following triangle of valuations

$$\begin{array}{cccccc}
Z^4 & \geq 0 & & & & \\
 & \geq 1 & \geq 0 & & & \\
 & = 1 & \geq 1 & \geq 0 & & \\
 & \geq 3 & \geq 2 & \geq 1 & \geq 0 & \\
X^4 & = 4 & \geq 3 & = 2 & \geq 2 & \geq 1 \quad Y^4
\end{array}$$

Now the reduction is $\overline{T} = zC_3(y, z)$, we cannot lift the points on $z = 0$. We split the computation in terms of the factorisation of $C_3$:

- is the null cubic with probability $\frac{1}{p^4}$;
- has a triple root different from $z = 0$ with probability $\frac{p-1}{p^3}$;
- is $z^3 = 0$, hence insolubility by primitivity, with probability $\frac{p-1}{p^4}$;
- is irreducible over $\mathbb{F}_p$, therefore insolubility, with probability $\frac{(p-1)(p^2-1)}{3p^3}$;
- has a linear factor, hence solubility, with probability $\frac{2p^4+p^3-2p^2-p}{3p^4}$.

Let us compute first the probability of solubility in the case of a triple root different from $z = 0$ we move it to $y = 0$ then, after the substitution $T(X, pY, Z)/p$ we have the following triangle of valuations

$$\begin{array}{cccccc}
Z^4 & \geq 0 & & & & \\
 & \geq 0 & \geq 1 & & & \\
 & = 0 & \geq 1 & \geq 2 & & \\
 & \geq 2 & \geq 2 & \geq 2 & = 2 & \\
X^4 & = 3 & \geq 3 & = 3 & \geq 4 & \geq 4 \quad Y^4
\end{array}$$

Table 8.3:

We have that the reduction is $z^2C_2(x, z) = 0$, but we cannot lift points on $z = 0$. $C_2(x, z)$ factors in the following ways:

- a double root, with probability $\frac{1}{p}$;
- no $\mathbb{F}_p$-rational root, with probability $\frac{p-1}{2p}$;
- two $\mathbb{F}_p$-rational roots, hence solubility, with probability $\frac{p-1}{2p}$.

In the first case we move the double root to $x = 0$ and, after the substitution $T(pX, Y, Z)/p$, we have the following triangle of valuations

$$\begin{array}{cccccc} Z^4 & \geq 0 & & & & \\ & \geq 1 & \geq 0 & & & \\ & = 1 & \geq 1 & \geq 1 & & \\ & \geq 4 & \geq 3 & \geq 2 & = 1 & \\ X^4 & = 6 & \geq 5 & = 4 & \geq 4 & \geq 3 \quad Y^4 \end{array}$$

With this reduction, if $v(a_{0,1,3}) = 0$ we have a linear factor and hence solubility, which happens with probability $\frac{p-1}{p}$. Otherwise, we can continue if the reduction is actually the null quartic, which happens with probability equal to $1/p^2$. After dividing by $p$ we get as reduction a cubic times the line $z = 0$, by interpolation we check that the cubic is irreducible and hence we have solubility.

Therefore, the probability of solubility in this case is

$$\psi = \frac{2p^4 + p^3 - 2p^2 - p}{3p^4} + \frac{\rho_1}{p^4} + \frac{p-1}{p^3}\left(\frac{p-1}{2p} + \frac{1}{p}\left(\frac{p-1}{p} + \frac{1}{p^2}\right)\right),$$

where $\rho_1 \in [0, 1]$ is the solubility in the case of the null cubic.

### Two conjugate lines

In the case of two conjugate lines whose interesection point is not in the line $z = 0$ we have a $\mathbb{F}_p$ singular point with two conjugate tangents, by the Proposition 7.3.2 we have that its solublity is $\frac{1}{p+1}$.

### Overall probability of solubility for the quadruple point

Gathering together the information

$$\frac{p^2-1}{p^3} + \frac{1}{p^4}\left(\frac{p-1}{p^6-1}\left(\theta p^2 + \psi p + \frac{p^4 - p^3}{2(p+1)} + \frac{p^4 + 2p^3 + 2p^2 + p}{2} + p^5 - p^2\right) + \frac{\rho_2}{p^6}\right),$$

where $\rho_2 \in [0,1]$ is the solubility in the case of the null conic.

We can rewrite it has

$$\begin{aligned}&24p^{22}+72p^{21}+96p^{20}+120p^{19}+156p^{18}+204p^{17}+216p^{16}+208p^{15}\\&+220p^{14}+191p^{13}+134p^{12}+66p^{11}+51p^{10}+48p^9-36p^8-48p^7\\&-28p^6-40p^5-44p^4-32p^3+12p^2-24\end{aligned}$$

divided by

$$24p^9(p+1)^2\left(p^2-p+1\right)\left(p^2+p+1\right)^2\left(p^6+p^3+1\right)$$

plus $\varepsilon$, where $\varepsilon \in \left[0, \frac{1+p+p^2+2p^3+p^4+p^5}{p^{10}(1+p+p^2+p^3+p^4+p^5)}\right]$ includes the possible values of $\rho_1$ and $\rho_2$.

We cannot compute the total solubility of this reduction since it is unclear whether there is any dependency between the liftability of the points in the double line and the one of the quadruple point. Since the latter is smaller than the former we can say that the probability of solubility of the curves having as reduction a product of a double line with two conjugate ones is at least greater or equal than $\chi$ stated in equation (8.5), which is when we take the limit of $p \to \infty$ is $5/8$. Moreover, we have that the overall probability of solubility is smaller than the sum of $\chi$ and the solubility of the quadruple point.

### 8.5.3 Two double lines

Another non-reduced case is when the reduction of the quartic is two double lines. We move them to $x^2y^2 = 0$ by a suitable change of coordinates. The triangle of valuations of the coefficients is:

$$\begin{array}{ccccccc}Z^4 & \geq 1 & & & & & \\ & \geq 1 & \geq 1 & & & & \\ & \geq 1 & \geq 1 & \geq 1 & & & \\ & \geq 1 & \geq 1 & \geq 1 & \geq 1 & & \\ X^4 & \geq 1 & \geq 1 & =0 & \geq 1 & \geq 1 & Y^4\end{array}$$

Here we have two different kind of singular points: the double ones, which are contained in one of the two lines (like $[1:0:0]$ or $[0:1:0]$), or the quadruple one $[0:0:1]$, which is the intersection of the two lines. Those points need a different treatment to work out the probability of lifting each of them, moreover we need to understand how the probability of lifting one single point could affect the probability of lifting others.

### Probability of lifting at least a double point

We denote with $\chi$ the probability of lifting at least one double point on the line $y = 0$. By the computation we are going to describe we understand that the probability of lifting a double point on $x = 0$ is independent of the lifting on points on $y = 0$, this comes from the fact that the procedure involves conditions on the valuations of disjoint sets. We pick the point $[1 : 0 : b]$ on the line $y = 0$ and we move it to $[1 : 0 : 0]$, by the change of coordinates that fixes $x$ and $y$ and sends $z$ to $z + bx$, we therefore have that $p|Y$ and $p|Z$. Since we want the probability of lifting at least one point we keep track of this change of coordinate, in certain configurations having the freedom to vary $b$ will guarantee solubility. In particular, we are interested in the new coefficients of some specific monomials after the change of coordinates, we have:

$$\begin{aligned} a'_{4,0,0} &= a_{4,0,0} + ba_{3,0,1} + b^2a_{2,0,2} + b^3a_{1,0,3} + b^4a_{0,0,4}, \\ a'_{3,0,1} &= a_{3,0,1} + 2ba_{2,0,2} + 3b^2a_{1,0,3} + 4b^3a_{0,0,4}, \\ a'_{3,1,0} &= a_{3,1,0} + ba_{2,1,1} + b^2a_{1,1,2} + b^3a_{0,1,3}, \\ a'_{2,2,0} &= a_{2,2,0} + ba_{1,2,1} + b^2a_{0,2,2}. \end{aligned} \tag{8.3}$$

All the valuation of the coefficients above are $\geq 1$ apart from $v(a_{2,2,0}) = 0$. Moreover, notice that $a'_{3,0,1}$ is the derivative in $b$ of $a'_{4,0,0}$. A necessary condition now is $p|Y$ and $p|Z$. After dividing through by $p$ the coefficient valuations will satisfy:

$$\begin{array}{cccccccc} Z^4 & \geq 4 & & & & & \\ & \geq 3 & \geq 4 & & & & \\ & \geq 2 & \geq 3 & \geq 4 & & & \\ & \geq 1 & \geq 2 & \geq 3 & \geq 4 & & \\ X^4 & \geq 0 & \geq 1 & = 1 & \geq 3 & \geq 4 & Y^4 \end{array}$$

By primitivity a necessary condition is $v(c(X^4)) > 0$, where $c(X^4) = a'_{4,0,0}/p$, the following steps rely on the possible factorisations of $f(b) = \overline{a'_{4,0,0}/p} \in \mathbb{F}_p[b]$, if for instance $f$ has only one root $\hat{b}$ this would mean that we can at most lift just one specific point on the line $y = 0$, the one which had initial coordinates $[1 : 0 : \hat{b}]$. Therefore, if $f(b)$ has no roots in $\mathbb{F}_p$ then none of the double points on $y = 0$ lift. Otherwise, if $f(b)$ has at least one root, since we are going to consider also the coefficient $a'_{3,0,1}$, which is linked to $a'_{4,0,0}$, we study the probability of solubility looking at both the coefficients at the same time. If the valuation $v(c(X^4))$ is strictly positive we have the following triangle of valuations:

$$\begin{array}{cccccc} Z^4 & \geq 3 & & & & \\ & \geq 2 & \geq 3 & & & \\ & \geq 1 & \geq 2 & \geq 3 & & \\ & \geq 0 & \geq 1 & \geq 2 & \geq 3 & \\ X^4 & \geq 0 & \geq 0 & = 0 & \geq 2 & \geq 3 \quad Y^4 \end{array}$$

If $v(c(X^3Z)) = 0$ (recall that $\overline{c(X^3Z)} = \overline{a'_{3,0,1}/p} = f'(b)$) we have a smooth conic times a line squared, therefore we would have a smooth point to lift, otherwise we have a binary monic quadratic form times a double line.

Recalling that $\overline{a'_{3,0,1}} = f'(b)$ is the derivative of $\overline{a'_{4,0,0}} = f(b)$ we describe the probabilities of each case above.

(i) $\exists b \in \mathbb{F}_p | f(b) = 0$ and $f'(b) \neq 0$, this happens if $f$ has a single root, by the difference with the other cases we have $(15p^5 - 5p^4 - p^3 - 19p^2 + 10p)/24$ cases.

(ii) $\forall b$ such that $f(b) = 0$ we have $f'(b) = 0$, then either $f$ is the null polynomial or it has only double roots. There are $\frac{p^4-p^3+5p^2-5p+2}{2}$ cases. Below we count these cases per number of double points.

(iii) $\forall b \in \mathbb{F}_p$ $f(b) \neq 0$, $f$ is either a non-zero constant ($p-1$ cases) or irreducible over $\mathbb{F}_p$ with degree at least 2 (respectively $(p-1)^2p/2$, $(p-1)\left(p^3 - p/3\right.$ and $(p-1)(p^4 - p^2)/4$ cases) or a product of irreducible quadrics $(p^5-3p^4+5p^3-5p^2+2p)/8$ cases). This leads to $(9p^5 - 7p^4 + 13p^3 - 41p^2 + 50p - 24)/24$ cases.

In case $(iii)$ we have no solubility. In case $(i)$, which happens with probability $(15p^5 - 5p^4 - p^3 - 19p^2 + 10p)/(24p^5)$, we have solubility 1.

In case $(ii)$ the quartic reduces to a double line times a binary quadratic

$$\overline{T} = X^2(X^2\overline{a'_{4,0,0}/p^2} + XY\overline{a'_{3,1,0}/p} + Y^2\overline{a'_{2,2,0}}), \tag{8.4}$$

with $\overline{a'_{2,2,0}} \neq 0$. By primitivity we cannot lift points on $x = 0$, therefore if the binary quadratic has a simple root we would have solubility since one of them would have non-zero $X$-coordinate, if the binary quadratic is irreducible over $\mathbb{F}_p$ there are no points to lift again by primitivity. If the quadratic has a double root, which cannot be $x = 0$ since $\overline{a'_{2,2,0}} \neq 0$, we may move it to $y = 0$. These informations are encoded in the Lagrange symbol of the discriminant $\Delta$ of the quartic. Indeed, if $\Delta$ is a non-zero quadratic residue we have 2 distinct roots, hence solubility. If $\Delta$ is zero we have a double root. If $\Delta$ is not a quadratic residue the quartic in (8.4) is irreducible over $\mathbb{F}_p$. Now we have:

| | | | | | | |
|---|---|---|---|---|---|---|
| $Z^4$ | $\geq 3$ | | | | | |
| | $\geq 2$ | $\geq 3$ | | | | |
| | $\geq 1$ | $\geq 2$ | $\geq 3$ | | | |
| | $\geq 1$ | $\geq 1$ | $\geq 2$ | $\geq 3$ | | |
| $X^4$ | $\geq 1$ | $\geq 1$ | $= 0$ | $\geq 2$ | $\geq 3$ | $Y^4$ |

Table 8.4: Quartic with solubility $\omega_2$.

At this stage we have a situation similar to the starting one, however due to the increase of some valuations the solubilities of these two configurations are different. Indeed, when we apply the same method used above, the coefficient $a'_{4,0,0}$ has at most degree 2 in $b$ when reduced mod $p$ instead of 4, this leads to different probabilities. Also, by primitivity, for solubility we must be able to lift a double point on $y = 0$ (and not on $x = 0$, which includes the quadruple point). Actually, there are no differences from the computation of the solubility $\omega_2$. Indeed, in the proof of the Lemma 7.3.8, we never took in consideration the coefficients of $C_4(Y, Z)$ since they have valuations greater or equal than 3 (in the aforementioned proof they had valuation at least 4, here they have valuation at least 3). Therefore, the solubility of this case is equal to $\omega_2$. Now we need to work out the probability that starting from a quartic in case $(ii)$ we end up in this configuration. We have $f(b) = 0$ and $f'(b) = 0$ then $b$ is a double root, since $f$ has degree at most 4 we can have either one or two double roots, we need to understand the probability that $f$ have either 1, 2 or $p$ (when $f(b)$ is identically zero) *distinct* roots. Let $R$ the set of roots of $f$.

$\#R = 2$ means that $f$ is a square of a polynomial of degree 2 with two distinct roots, this give us $p(p-1)^2/2$ cases. $\#R = 1$ happens when $f$ is either a square or a cube or a forth power of a linear equation ($3p(p-1)$ cases) or if it is a square of a linear one times an irreducible ($p^2(p-1)^2/2$ cases). $\#R = p$ happens only if $f$ is identically zero. Summarising we have:

| $\#R$ | $p$ | 1 | 2 |
|---|---|---|---|
| $p^5 \cdot \mathbb{P}(f \text{ has no simple roots} \wedge \#R = t)$ | 1 | $(p^4 - 2p^3 + 7p^2 - 6p)/2$ | $p(p-1)^2/2$ |

In particular we need to subdivide the case $R = 1$ by the multiplicity of the root

| Multiplicity | Double | Triple | Quadruple |
|---|---|---|---|
| $p^5 \cdot \mathbb{P}(f \text{ has no simple roots} \wedge \#R = 1)$ | $(p^4 - 2p^3 + 3p^2 - 2p)/2$ | $p(p-1)$ | $p(p-1)$ |

Indeed, the valuations are not identical for the cases above. When $f$ has a double root or two double roots the triangle of valuations is the one described in Table 8.5.3, in

other cases the first column changes slightly. Indeed, assuming $p$ different from 2 and 3, if $f$ has a quadruple root the first column is

$$Z^4 \quad \geq 3 \quad \geq 3 \quad \geq 2 \quad \geq 1 \quad \geq 1 \quad X^4$$

which has solubility $\chi_3$. If $f$ has a triple root, assuming $p \neq 2$, the first column is

$$Z^4 \quad \geq 3 \quad \geq 2 \quad \geq 2 \quad \geq 1 \quad \geq 1 \quad X^4$$

and leads to solubility $\chi_2$. Lastly, if $f$ is the null polynomial, the first column is

$$Z^4 \quad \geq 4 \quad \geq 3 \quad \geq 2 \quad \geq 1 \quad \geq 1 \quad X^4$$

which has solubility $\chi_3$.

Now we compute for each of the 3 possible cardinalities of $R$ what are the probabilities of solubility, insolubility or ending in the configuration with solubility probability $\omega_2$. The reduction is the one described above in (8.4), where $h(b) = \overline{a'_{4,0,0}/p^2}$ has degree at most 4, $g(b) = \overline{a'_{3,1,0}/p}$ has degree at most 3 and $\overline{a'_{2,2,0}}$ is constant and non-zero. $h$ and $g$ have random coefficients, which are independent and uniformly distributed over $\mathbb{F}_p$, therefore the discriminant $\Delta(b) = g(b)^2 - 4h(b)\overline{a'_{2,2,0}}$ of the quadratic form in (8.4) has the first 5 coefficients uniformly distributed. It follows that we can apply Proposition 7.2.2 which implies that $\Delta(b_i)$ are uniformly and independently distributed when $b_i \in R$ and $\#R \leq 5$. We have solubility when $\Delta(b_i)$ is a non-zero quadratic residue for at least one element of $R$, we end up in the configuration with solubility $\omega_2$ if $\Delta(b_i)$ is never a non-zero quadratic residue for all $i$ but it assumes the value 0 at least once. We have that

$$\mathbb{P}\left(\left(\frac{\Delta(b_0)}{p}\right) = 1\right) = \frac{p-1}{2p} = \psi,$$

from which, by inclusion and exclusion, we work out the following

| | $\#R = 1$ | $\#R = 2$ |
|---|---|---|
| Solubility 1 | $\psi = \frac{p-1}{2p}$ | $1 - (1-\psi)^2 = \frac{3p^2-2p-1}{4p^2}$ |
| $\omega_2$ or $\chi_2$ or $\chi_3$ | $1 - 2\psi = \frac{1}{p}$ | $1 - 2\psi = \frac{1}{p}$ |
| Solubility 0 | $\psi = \frac{p-1}{2p}$ | $\psi^2 = \left(\frac{p-1}{2p}\right)^2$ |

It remains to study the case when $\#R = p$, here we need to study the probability that $\Delta(b)$ has a certain degree and leading coefficient, then we can use the Lemma 7.2.1.

Considering the discriminant $\Delta(b) = g(b)^2 - 4h(b)\overline{a'_{2,2,0}}$ we have that the first 5 coefficients $\Delta_0, \ldots, \Delta_4$ are uniformly and independently distributed, $\Delta_5$ and $\Delta_6$ are not independent but the latter is non-zero if and only if $g_3 \neq 0$. Therefore, if $g_3 \neq 0$, then $\Delta(b)$ is a degree 6 polynomial with leading coefficient a quadratic residue. Otherwise, if $g_3 = 0$ $\Delta(b)$ is a polynomial of degree at most 4 whose coefficients are all independent and uniformly distributed over $\mathbb{F}_p$. Using this information together with the Lemma 7.2.1 we have the following table.

| $\deg(\Delta)$ | $\mathbb{P}(\deg(\Delta) = t)$ | Solubility 1 | Solubility $\chi_3$ | Solubility 0 |
|---|---|---|---|---|
| 6 | $\frac{p-1}{p}$ | 1 | 0 | 0 |
| 4 | $\frac{p-1}{p^2}$ | $\frac{2p^2-1}{2p^2}$ | $\frac{p+1}{4p^3}$ | $\frac{p-1}{4p^3}$ |
| 3 | $\frac{p-1}{p^3}$ | 1 | 0 | 0 |
| 2 | $\frac{p-1}{p^4}$ | $\frac{2p-1}{2p}$ | $\frac{1}{2p}$ | 0 |
| 1 | $\frac{p-1}{p^5}$ | 1 | 0 | 0 |
| 0 | $\frac{1}{p^5}$ | $\frac{p-1}{2p}$ | $\frac{1}{p}$ | $\frac{p-1}{2p}$ |

Recall that $\chi$ is the probability that at least one of the double points on the line $y = 0$ (but not the quadruple one $[0:0:1]$) lifts, summarizing all the information above we have:

$$\begin{aligned}\chi =& \frac{15p^5 - 5p^4 - p^3 - 19p^2 + 10p}{24p^5} + \\ & \frac{1}{p^5}\left[\frac{p-1}{p} + \frac{p-1}{p^2}\left(\frac{2p^2-1}{2p^2} + \frac{p+1}{4p^3}\chi_3\right) + \frac{p-1}{p^3} + \right. \\ & \frac{p-1}{p^4}\left(\frac{2p-1}{2p} + \frac{1}{2p}\chi_3\right) + \frac{p-1}{p^5} + \frac{1}{p^5}\left(\frac{p-1}{2p} + \frac{1}{p}\chi_3\right) + \\ & \frac{p^4 - 2p^3 + 3p^2 - 2p}{2}\left(\frac{p-1}{2p} + \frac{\omega_2}{p}\right) + \left(\frac{p(p-1)^2}{2}\right)\left(\frac{3p^2 - 2p - 1}{4p^2} + \frac{\omega_2}{p}\right) \\ & \left. + p(p-1)\left(\frac{p-1}{2p} + \frac{\chi_2}{p}\right) + p(p-1)\left(\frac{p-1}{2p} + \frac{\chi_3}{p}\right)\right].\end{aligned}$$

By the expression of $\omega_2$, $\chi_2$ and $\chi_3$ from the Corollary 7.3.12, we compute the rational function for $\chi$ as well. The numerator of $\chi$ is

$$\begin{aligned}&30p^{17} + 32p^{16} - 6p^{15} + 29p^{14} + 25p^{13} - 27p^{12} + 55p^{11} + 171p^{10} - 245p^9 + 90p^8 \\ &+ 78p^7 - 79p^6 - 15p^5 - 6p^4 + 90p^3 - 120p^2 + 48p - 6\end{aligned} \tag{8.5}$$

and the denominator is $24p^{10}\left(p\left(p(p+1)\left(2p^4+p+1\right)-1\right)+2\right)$. Since our methods to compute $\chi$ involved just the study of the coefficients of the terms $X^4, X^3Z$ and $X^3Y$, in order to compute the probability of solubility for the double points on $x=0$ we would look at the coefficients of the terms $Y^4, Y^3Z$ and $Y^3Z$, since the two sets are disjoint the two solubilities are independent. Therefore, we have that the total solubility for the double points is $1-(1-\chi)^2$, whose numerator is

$$1980p^{34}+4032p^{33}+1832p^{32}+2292p^{31}+6208p^{30}+4400p^{29}+1487p^{28}+11182p^{27}$$
$$+4109p^{26}-5108p^{25}+3127p^{24}+20354p^{23}-5117p^{22}-45012p^{21}+42311p^{20}+49010p^{19}$$
$$-104209p^{18}+34568p^{17}+57036p^{16}-45004p^{15}-21930p^{14}+13524p^{13}+62603p^{12}$$
$$-87294p^{11}+31383p^{10}+21180p^9-22704p^8+6000p^7-9048p^6+21996p^5-23112p^4$$
$$+12600p^3-3744p^2+576p-36$$

and the denominator is

$$576p^{20}\left(p\left(p(p+1)\left(2p^4+p+1\right)-1\right)+2\right)^2.$$

### Probability of lifting the quadruple point

The coordinates of the quadruple point are $[0:0:1]$, therefore in order to try to lift it we make the substitution $T \to T(pX,pY,Z)/p$. The reduction we obtain is $\overline{a_{4,0,0}}z^4=0$. By primitivity, we have insolubility if $\overline{a_{4,0,0}}\neq 0$, then we can continue if and only if $\overline{a_{4,0,0}}$ is zero, which happens with probability $\frac{1}{p}$. Dividing by $p$ we obtain as reduction

$$C_1(x,y)z^3+C_0(x,y)z^4.$$

If $C_1$ is not null the reduction contains a reduced line different from $z=0$, which implies that the point lifts; this happens with probability $\frac{p^2-1}{p^2}$. Otherwise, when the quartic is null, we make a further step to compute the solubility; this happens with probability $\frac{1}{p^3}$.

Dividing by $p$ the reduction is a double line times a generic quartic $\gamma$. We distinguish, as usual, the reductions of $\gamma$ by the probability of solubility.

- The cases with solubility equal to 1 are: a smooth conic or two $\mathbb{F}_p$-lines. It happens with probability $\frac{2p^5+p^4+2p^3+p}{2(p^5+p^4+p^3+p^2+p+1)}$.
- The cases with solubility equal to 0 are: the double line $z^2=0$ and a product of

two conjugate $\mathbb{F}_{p^2}$-lines whose intersection is in the line $z = 0$. It happens with probability $\frac{p^3-p+2}{2(p^5+p^4+p^3+p^2+p+1)}$.

- The case with solubility equal to $\frac{1}{p+1}$, by the Proposition 7.3.2: a product of two conjugate $\mathbb{F}_{p^2}$-lines whose intersection is in the line $z = 0$. This happens with probability $\frac{p^4-p^3}{2(p^5+p^4+p^3+p^2+p+1)}$.
- The case with undetermined solubility: a line squared different from $z^2 = 0$. This happens with probability $\frac{p^2+p}{p^5+p^4+p^3+p^2+p+1}$.

It follows that the probability of lifting the quadruple point is

$$\frac{2p^8 + 4p^7 + 2p^6 + 2p^5 + 3p^4 + 4p^3 - p^2 - 3p - 1}{2p^3(p+1)^2\left(p^4 + p^2 + 1\right)},$$

plus $\epsilon$, where $\epsilon \in \left[0, \frac{1}{p^7+p^5+p^3}\right]$.

### Overall probability of solubility for the two double lines

It is intricate to compute the correlation between the probability of solubility of the double points and the one of the quadruple points. In case we have that the overall probability will be greater than or equal to the maximum of above mentioned probabilities and it is smaller than or equal to the sum of the two probabilities. Therefore, a lower bound for the overall solubility is the probability of solubility of the double points, since for $p$ big enough it is the maximum of the two probabilities, the upper bound is given by the sum of the terms with $\epsilon$ maximal. The numerator of the upper bound is

$1980p^{40} + 10296p^{39} + 23072p^{38} + 31804p^{37} + 40304p^{36} + 58976p^{35} + 77859p^{34} + 85092p^{33} + 88183p^{32} + 96308p^{31} + 92739p^{30} + 90348p^{29} + 93650p^{28} + 40932p^{27} + 14300p^{26} + 89052p^{25} + 40442p^{24} - 54984p^{23} + 12455p^{22} + 69720p^{21} + 9807p^{20} - 95104p^{19} + 34782p^{18} + 80884p^{17} - 67783p^{16} - 27252p^{15} + 38158p^{14} + 29860p^{13} - 49315p^{12} - 11676p^{11} + 43119p^{10} - 19956p^9 - 9576p^8 + 3960p^7 + 7548p^6 - 5436p^5 - 4320p^4 + 6192p^3 - 2664p^2 + 504p - 36$

while the denominator is

$$576p^{20}(p+1)^2\left(p^3 - p + 1\right)^2\left(p^4 + p^2 + 1\right)\left(2\left(p^2 + p + 1\right)p^2 + p + 2\right)^2.$$

The difference between the two bounds is roughly $\frac{1}{p}$.

### 8.5.4 Quadruple line

When the reduction of the quartic is a quadruple line we have $p+1$ singular points in $\mathbb{P}^2(\mathbb{F}_p)$ that may lift. As described in the other sections it is difficult to understand the correlations between the probability of liftability of each point, in order to compute the overall probability of solubility.

We change the coordinates in such a way the reduction is $x^4 = 0$. The first substitution is $T \to T(pX, Y, Z)/p$, which give us as reduction a binary quartic $C_4(y, z)$. The possible factorisation and their associated probabilities are described in the Corollary 5.3.4, recapping we have:

- Irreducible over $\mathbb{F}_p$, therefore there are no point to lift by primitivity. This happens with probability equal to $\frac{3p^4-5p^3+3p^2-3p+2}{8p^4}$.
- It has at least one single root, in this case it lifts and we have solubility. This happens with probability equal to $\frac{5p^4+p^3-3p^2-p-2}{8p^4}$.
- Just one double root. This happens with probability equal to $\frac{p^3-p^2-p+1}{2p^4}$.
- Two double roots. This happens with probability equal to $\frac{p^2-1}{2p^4}$.
- A quadruple root. This happens with probability equal to $\frac{p^2-1}{p^5}$.
- The null quartic. This happens with probability equal to $\frac{1}{p^5}$.

The last 4 cases are undetermined.

#### One and two double roots cases

First we deal with the single double root case. We move it to $y = 0$. After the substitution $T \to T(X, pY, Z)/p$ the reduction is $\overline{a_{0,0,4}}z^4 + \overline{a_{1,0,3}}xz^3$. If $\overline{a_{1,0,3}} \neq 0$ we have a linear factor that is different from $z$, hence solubility, this happens with probability $\frac{p-1}{p}$. Otherwise, if $\overline{a_{1,0,3}} = 0$, we have insolubility, by primitivity, if $\overline{a_{0,0,4}} = 0$. The indeterminate case is when the reduction is the null quartic, which happens with probability $\frac{1}{p^2}$. Dividing all the coefficients by $p$ we have the following triangle of valuations

$$\begin{array}{cccccc} Z^4 & \geq 0 & & & & \\ & \geq 0 & \geq 0 & & & \\ & \geq 0 & \geq 0 & = 0 & & \\ & \geq 1 & \geq 1 & \geq 1 & \geq 1 & \\ X^4 & = 1 & \geq 2 & \geq 2 & \geq 2 & \geq 2 \quad Y^4 \end{array}$$

The probability of solubility of this case has been already studied in the proof of the Proposition 8.1.3 and its value $\tau$ is computed in the equation (8.1). It follows that the solubility of this case is $\frac{p-1}{p} + \frac{\tau}{p^2}$. When we have two double roots the solubility can be computed in function of the one with one double root, and we have

$$1 - \left(1 - \frac{p-1}{p} + \frac{\tau}{p^2}\right)^2 = \frac{p^4 - p^2 + 2p\tau - \tau^2}{p^4}.$$

### Quadruple root case

In the case we have a quadruple root we move it to $y = 0$. Making the same steps we did for the double root we obtain solubility equal to $\frac{p-1}{p} + \frac{\theta}{p^2}$, where $\theta$ is the probability of solubility of the quartic having as triangle of valuations

$$\begin{array}{cccccc} Z^4 & \geq 0 & & & & \\ & \geq 0 & \geq 0 & & & \\ & \geq 0 & \geq 0 & \geq 1 & & \\ & \geq 1 & \geq 1 & \geq 1 & \geq 2 & \\ X^4 & = 1 & \geq 2 & \geq 2 & \geq 2 & = 2 \quad Y^4 \end{array}$$

This reduction has a smooth point, and hence solubility, in $p^5 - p^3/2 - p/2$ cases, in the remaining ones its undetermined. Then we can say that

$$\frac{2p^5 - p^3 - p}{2p^5} \leq \theta \leq 1.$$

### Null quartic case

In the case the reduction is the null quartic we have, after dividing by $p$, as reduction

$$C_3(y, z)x + C_4(y, z).$$

If $C_3(y, z) \neq 0$ in $[1 : 0 : 0]$ we have a triple point. Considering the lines through the point, by Bézout's Theorem, either they intersect the quartic in a forth smooth point or the quartic contains the line. Since we have $p + 1$ lines to consider, either the quartic contains a reduced line or a smooth point, in both cases we have solubility. Otherwise, with probability $1/p^4$ we are back to studying the quartic.

The possible factorisations of the quartic are the ones described in Corollary 5.3.4. We have solubility equal 1 with probability $\frac{3p^4-5p^3+3p^2-3p+2}{8p^4}$; solubility 0 with probability equal to $\frac{5p^4+p^3-3p^2-p-2}{8p^4}$. It is undetermined in all the other cases. This give us bounds on the solubility of this reduction that we can use to compute the overall solubility.

### Overall probability of solubility for the quadruple line

Summarising we have that the solubility of a quadruple line can be estimated by an upper and lower bound. The numerator of the lower bound is

$48p^{30}+128p^{29}+176p^{28}+352p^{27}+480p^{26}+608p^{25}+1000p^{24}+1328p^{23}+1416p^{22}+1368p^{21}+1144p^{20}+920p^{19}+567p^{18}+293p^{17}+12p^{16}-738p^{15}-1366p^{14}-1628p^{13}-1669p^{12}-1383p^{11}-1152p^{10}-944p^{9}-768p^{8}-640p^{7}-256p^{6}+64p^{5}+192p^{4}+240p^{3}+128p^{2}+48p+32$

and its denominator is

$$128p^{13}(p+1)\left(p^2+p+1\right)^2\left(p^6+p^3+1\right)^2.$$

The numerator of the upper bound is

$48p^{30}+128p^{29}+176p^{28}+352p^{27}+480p^{26}+608p^{25}+1000p^{24}+1392p^{23}+1608p^{22}+1688p^{21}+1656p^{20}+1624p^{19}+1463p^{18}+1445p^{17}+1420p^{16}+926p^{15}+426p^{14}+164p^{13}+123p^{12}+281p^{11}+384p^{10}+464p^{9}+384p^{8}+256p^{7}+384p^{6}+512p^{5}+512p^{4}+432p^{3}+256p^{2}+112p+32$ and its denominator is

$$128p^{13}(p+1)\left(p^2+p+1\right)^2\left(p^6+p^3+1\right)^2.$$

The difference between the two bounds is roughly $\frac{1}{2p^7}$.

### 8.5.5 Conic squared

When a quartic has as reduction on $\mathbb{F}_p$ a conic squared it is really complicated to study its probability of solubility. We have $p+1$ double points and it is already problematic to describe the liftability of one single point, but this would not describe the overall solubility of this case. We have to compute the correlation between the solubilities of all the double points, but all the previous techniques look powerless in this setting: when we were considering the product of two double lines we were able to change the coordinates in such a way we could control which point lift without changing the reduction: here, such a change of coordinates would change drastically the equation of the reduction, without chance of tracking the correlation between the solubilities of the points.

In this case we just give an estimate of the probability of liftability of a fixed point. As standard model for an irreducible conic we use $y^2+xz=0$. So we can write a squared conic as $y^2+2xy^2z+x^2z^2$.

All the $p+1$ points on the reduction are double ones; they are $[1:0:0]$, $[0:0:1]$ and for all $t\in\mathbb{F}_p^*$ $[t:1:(-t)^{-1}]$. We want to compute the probability to lift the first

point. We estimate the probability of lifting the point $[0:0:1]$. As first step we make the substitution $T \to T(pX, pY, Z)$, which gives us the reduction $\overline{a_{0,0,4}}z^4 = 0$. By primitivity, we can continue if and only if $\overline{a_{0,0,4}} = 0$, which happens with probability $\frac{1}{p}$. After dividing by $p$ we get the reduction $z^2(x^2+axz+bz^2+cyz) = 0$. If $c \neq 0$, the monic conic is irreducible, since its determinant it not null, hence it has at least a smooth point that is not on $z = 0$ and so we have solubility; this happens with probability $(p-1)/p$. Otherwise, with probability $1/p$, $c = 0$ which leads us to the following factorisations of the term $(x^2 + axz + bz^2)$:

- two conjugate roots, with probability equal to $(p-1)/2p$, but this would imply $p|Z$, which is impossible by primitivity so there would be no point to lift;
- a double root, with probability equal to $1/p$;
- two solutions, with probability equal to $(p-1)/2p$, then, since they cannot have the $z$ coordinate equal to 0, we can lift them and conclude.

The only undetermined case is the second one, after a suitable change of coordinates we assume the double line to be $x = 0$. Let us analyse the change of coordinates: starting from the double line $x - \alpha z{=}0$ we fix $y$ and $z$ and map $x$ to $x + \alpha z$. Notice that the coefficients of $x^2z^2$, $xy^2z$ and $y^4$ do not change their valuations after the change of coordinates. Indeed, the coefficient of $x^2z^2$ is set to be 1 mod $p$ by the change of coordinates, the one of $y^4$ is not affected by the change of coordinates and the coefficient of $xy^2z$ is $2a_{220}\alpha + a_{121}$, but the valuation of $2a_{220}$ is $\geq 3$, while the other term has valuation equal to 1, therefore the sum has valuation equal to 1. Summing up, after the change of coordinates and the substitution $T \to T(pX, Y, Z)/p$ the triangle of valuations of the quartic is

$$\begin{array}{ccccccc}
Z^4 & \geq 0 & & & & & \\
 & \geq 1 & \geq 0 & & & & \\
 & = 1 & \geq 1 & \geq 0 & & & \\
 & \geq 4 & \geq 3 & = 1 & \geq 1 & & \\
X^4 & \geq 6 & \geq 5 & \geq 4 & \geq 3 & = 1 & Y^4
\end{array}$$

With probability $(p-1)/p$ the coefficient of $y^2z^2$ is not zero, then, by Proposition 8.1.1, the probability of solubility is 1/2. In the case $\overline{a_{0,2,2}} = 0$ and $\overline{a_{0,1,3}} \neq 0$, which happens with probability $(p-1)/p^2$, we have a line times a triple line, so it has solubility equal to 1. If $\overline{a_{0,2,2}} = \overline{a_{0,1,3}} = 0$ and $\overline{a_{0,0,4}} \neq 0$, which happens with probability equal

to $(p-1)/p^3$, the solubility is 0 by primitivity. In the case of a null quartic, probability equal to $1/p^3$, we should continue the investigation further.

Assuming the reduction is the null quartic, dividing by $p$, this is the triangle of the valuations of the quartic

$$\begin{array}{cccccc} Z^4 & \geq 0 & & & & \\ & \geq 0 & \geq 0 & & & \\ & = 0 & \geq 0 & \geq 0 & & \\ & \geq 3 & \geq 2 & = 0 & \geq 0 & \\ X^4 & \geq 5 & \geq 4 & \geq 3 & \geq 2 & = 0 \quad Y^4 \end{array}$$

where the coefficients of $x^2z^2$, $xy^2z$ and $y^4$ are the same set at the beginning.

About this family of quartics we know that they have a singular point in $[1:0:0]$ with double tangent $z=0$. By primitivity we cannot lift this point. By interpolation on the small primes we have the counts of the possible reduction of these quartics, in total there are $p^6$ of them.

- $p^6 - p^4$ are irreducible, by (8.2) if the cardinality of the base field is bigger than 19 we have solubility equal to 1.
- $p^2(p^2-1)/2$ are conjugate conics, which are divided in:
  - $p^2(p-1)/2$ which have just one point with multiplicity of the intersection equal to 4, which is the point we cannot lift by primitivity, so in this case we have insolubility.
  - $p^2(p^2-p)/2$ which have 2 points with multiplicity of the intersection equal to 3 and 1; we cannot lift the one with multiplicity 3 but the other one is not in the line $z=0$, therefore the solubility of this case is equal to the solubility of the conjugate conic having just one point with multiplicity 1. By Section 7.4.1 the solubility is $1/(p+1)$.
- $p^2(p^2+1)/2$ are a product of two irreducible conics and they split in:
  - $p^2$ irreducible conics square, from those we can lift any point but $[1:0:0]$, we denote the solubility of this case by $\theta$.
  - $p^2(p^2-1)/2$ distinct irreducible conics, which for $p>3$ have at least one smooth point, therefore we have solubility.

Computing the solubility $\theta$ is the remaining and hard part of this procedure. Is unclear how to achieve it since, as said above, we have no tools to study efficiently the corrections between the liftabilities of the double points. Some numerical experiments on the distribution on the number of points of the reduction that do lift suggest a behaviour similar to a binomial distribution, which would mean an independency between the liftabilities of each point. This would imply an exponential formula that describes the probability overall of solubility of the quartics having as reduction a conic squared, in contrast with all other probabilities that are described by a rational function.

In any case, we can give an estimate by lower and upper bounds on the probability of lifting one point of the conic squared. The lower bound is, of course, also a lower bound for the solubility overall of the conic squared case.

The lower bound is

$$\frac{2p^{10}+p^9-p^8+p^7-p^6+2p^4-p^3-2p-1}{2p^{10}(p+1)},$$

while the upper bound is

$$\frac{2p^{10}+p^9-p^8+p^7-p^6+2p^4-p^3+1}{2p^{10}(p+1)}.$$

The difference between the two bounds is $\frac{1}{p^{10}}$.

# Chapter 9

# Formulas and estimates for the density of everywhere locally solvable plane quartics

Taking into account the results obtained in the previous chapters we now describe the portion of everywhere locally solvable plane quartics. We start by summarizing the information we have.

By Theorem 3.2.3 we express the probability $\rho$ that a random integral plane quartic is everywhere locally solvable as

$$\rho = \rho(\mathbb{R}) \prod \rho(\mathbb{Q}_p),$$

where random means uniformly distributed on the unit hypercube in the space of the coefficients and $\rho(K)$ is the probability that a random rational plane quartic is solvable over the field $K$.

In Section 4.3 we discussed bounds and estimates for $\rho(\mathbb{R})$, namely we have

$$0.975068161914319 \leq \rho(\mathbb{R}) \leq 0.9999999684,$$

and numerical evidence suggests that in fact,

$$\rho(\mathbb{R}) \simeq 0.9792.$$

Now we describe in detail the computation of the local solubility $\rho(\mathbb{Q}_p)$.

## 9.1 The probability $\rho(\mathbb{Q}_p)$ of local solubility

In order to compute $\rho(\mathbb{Q}_p)$ we use the results from Chapters 5, 7 and 8; we recap them in the tables below. The first table is organised as follows: in the first column we describe the type of reduction; in the second column the cardinality of curves over $\mathbb{F}_p$ per type; in the third column the probability of solubility (if it is 1 or 0 we state it, otherwise we refer to the section were we computed it); in the fourth column we give the minimum prime $p_0$ for which we have proved the formula of the probability of solubility; in the last one we indicate whether the reduction can be semi-stable.

| Reduction | Cardinality | Sol. | $p_0$ | Semi |
|---|---|---|---|---|
| **Four $\mathbb{F}_p$-lines** | | | | |
| $L^4$ | $p^2+p+1$ | 8.5.4 | 2 | |
| $L_1^3 \cdot L_2$ | $p(p+1)(p^2+p+1)$ | 1 | 2 | |
| $L_1^2 \cdot L_2 \cdot L_3$ | $p(p+1)(p^2+p+1)(p^2+p-1)/2$ | 1 | 2 | |
| $L_1^2 \cdot L_2^2$ | $p(p+1)(p^2+p+1)/2$ | 8.5.3 | 19 | |
| $L_1 \cdot L_2 \cdot L_3 \cdot L_4$ | $p(p+1)(p^2+p+1)(p^2+p-1)(p^2+p-2)/24$ | 1 | 2 | ✓ |
| **Two $\mathbb{F}_p$-lines times two conjugate $\mathbb{F}_{p^2}$-lines** | | | | |
| $L_1 \cdot L_2 \cdot L_3 \cdot \sigma(L_3)$ | $p^2(p^2-1)(p^2+p+1)^2/4$ | 1 | 2 | ✓ |
| $L_1^2 \cdot L_2 \cdot \sigma(L_2)$: | | | | |
| •w/o quadruple; | $p^3(p-1)(p^2+p+1)$ | 8.5.1 | 2 | |
| •with quadruple. | $p(p-1)(p+1)(p^2+p+1)$ | 8.5.2 | 2 | |
| **Two pairs of conjugate $\mathbb{F}_{p^2}$-lines** | | | | |
| $(L \cdot \sigma(L))^2$ | $p(p-1)(p^2+p+1)/2$ | 8.4.1 | 2 | |
| $\sigma(L_1) \cdot L_2 \cdot \sigma(L_2)$: | | | | |
| •w/o quadruple; | $(p^4-p)(p^2-p)(p^2+p)/8$ | 7.4.2 | 2 | ✓ |
| •with quadruple. | $(p^2+p+1)(p^2-p)(p^2-p-2)/8$ | 8.4.1 | 2 | |
| $L_1 L_2 \sigma_3(L_2) \sigma_3^2(L_2)$ | $(p-1)p(p+1)(p^3+p+1)(p^2+p+1)/3$ | 1 | 2 | ✓ |
| **Four $\mathbb{F}_{p^4}$-lines** | | | | |
| •Concurrent; | $(p^2+p+1)(p^4-p)/4$ | 8.4.1 | 2 | |
| •w/o $\mathbb{F}_p$-points. | $(p^8-p^6-p^5-p^4+p^3+p)/4$ | 0 | 2 | |
| **An irreducible conic times two lines** | | | | |
| $L_1 \cdot L_2 \cdot Q$ | $p^3(p-1)(p+1)(p^2+p+1)^2/2$ | 1 | 2 | ✓ |
| $L_1^2 \cdot Q$ | $(p^2+p+1)(p^5-p^2)$ | 1 | 2 | |
| $L \cdot \sigma(L) \cdot Q$ | $p^3(p-1)^2(p^2+p+1)^2/2$ | 1 | 2 | ✓ |
| **Two $\mathbb{F}_p$-conics** | | | | |
| $Q_1 \cdot Q_2$ | $(p^5-p^2)(p^5-p^2-1)/2$ | 1 | 3 | ✓ |
| $Q^2$ | $p^5-p^2$ | 8.5.5 | 19 | |
| $T = L \cdot C$ | $p^5(p^2-1)(p^2+p+1)^2$ | 1 | 3 | ✓ |
| **Two conjugate $\mathbb{F}_{p^2}$-conics** | | see Table 9.2 | | |
| **Absolutely irreducible quartics** | | see Table 9.3 | | |

Table 9.1: Solubilities for all the reduction types

We recall in the following Table 9.2 the possible sub-cases of the product of two conjugate $\mathbb{F}_{p^2}$-conics. Here the first column describes the intersection multiplicities of the $\mathbb{F}_p$-points; the remaining columns are the same as in Table 9.1.

| $I_p(\gamma,\overline{\gamma})$ | Cardinality | Sol. | $p_0$ | Semi |
|---|---|---|---|---|
| 0 | $(3p^{10}-3p^9-3p^8-4p^7+7p^6+3p^5+p^4-4p^3)/16$ | 0 | 2 | ✓ |
| 1 | $(p^{10}-p^9-p^8+p^6+p^5-p^4)/6$ | 7.4.1 | 2 | ✓ |
| 2 | $(p^9-p^7-p^6+p^4)/4$ | 8.3.1 | 19 | |
| 4 | $(p^7-p^5-p^4+p^2)/2$ | 8.3.5 | 19 | |
| 1,1 | $(p^{10}-p^9-3p^8+3p^6+3p^5-p^4-2p^3)/8$ | 7.4.1 | 2 | ✓ |
| 2,2 | $(p^8+p^7-p^5-p^4)/4$ | 8.3.2 | 19 | |
| 1,3 | $(p^8-p^6-p^5+p^3)/2$ | 8.3.4 | 19 | |
| 1,1,2 | $(p^9-p^7-p^6+p^4)/4$ | 8.3.3 | 19 | |
| 1,1,1,1 | $(p^{10}-p^9-p^8+p^6+p^5-p^4)/48$ | 7.4.1 | 2 | ✓ |

Table 9.2: Solubilities for Conjugate Conics

Table 9.3 regards the absolutely irreducible quartics; the first column describes the singularities of the curve: by the notation $[r,s,t]$ we mean a quartic that has $r$ double points defined over $\mathbb{F}_p$, $s$ on $\mathbb{F}_{p^2}$ but not on $\mathbb{F}_p$ and $t$ on $\mathbb{F}_{p^3}$ but not on $\mathbb{F}_p$. The only case left by this notation is the triple $\mathbb{F}_p$-point. In Section 8.2 there is the discussion about the $p_0$ associated to these reductions.

| Type Singularities | Cardinality | Sol. | $p_0$ | Semi |
|---|---|---|---|---|
| $[0,0,0]$ | $p^{14}-p^{12}-p^{11}+p^9+p^8-p^6-p^5+p^3$ | 1 | 31 | ✓ |
| $[1,0,0]$ | $p^3(p^{10}+p^9-2p^7-2p^6-p^5+p^4+2p^3+p^2-1)$ | 1 | 19 | ✓ |
| $[2,0,0]$ | $(p^{12}+p^{11}-2p^9-p^8+p^3)/2$ | 1 | 11 | ✓ |
| $[0,2,0]$ | $p^3(p^9-p^8-p^5+2p^2-1)/2$ | 1 | 7 | ✓ |
| $[3,0,0]$ | $(p^{11}-p^{10}-p^9-p^8+p^7+2p^6-p^3)/6$ | 1 | 7 | ✓ |
| $[1,2,0]$ | $(p^{11}-p^{10}-p^9+p^8+p^7-2p^5+p^3)/2$ | 1 | 5 | ✓ |
| $[0,0,3]$ | $(p^{11}-p^{10}-p^9-p^8+p^7+2p^6-p^3)/3$ | 1 | 3 | ✓ |
| One triple $\mathbb{F}_p$-point | $p^{10}+p^9-p^7-p^6$ | 1 | 3 | |

Table 9.3: Solubilities for Absolutely Irreducible Quartics

The total number of plane quartics defined over $\mathbb{F}_p$ is $(p^{15}-1)/(p-1)$. Weighting the cardinality of each reduction with the associated probability of solubility and dividing

by the total number of curves we compute $\rho(\mathbb{Q}_p)$. We describe $\rho(\mathbb{Q}_p)$ for $p$ greater or equal than the maximum of all the $p_0$, which is 31. Since for some probability of solubility we have just lower and upper bounds we cannot state the exact formula, but we can still provide quite sharp bounds.

The numerator of the lower bound of $\rho(\mathbb{Q}_p)$, for $p \geq 31$, is

$9216p^{84}+73728p^{83}+285696p^{82}+764928p^{81}+1686528p^{80}+3331584p^{79}+6081408p^{78}+10374528p^{77}+16704960p^{76}+25653504p^{75}+37798968p^{74}+53647752p^{73}+73666288p^{72}+98167792p^{71}+127255052p^{70}+160779768p^{69}+198238532p^{68}+238926716p^{67}+281953118p^{66}+326080398p^{65}+369600258p^{64}+410820754p^{63}+448446635p^{62}+480715442p^{61}+505760928p^{60}+522481619p^{59}+530102379p^{58}+528015408p^{57}+515844422p^{56}+494144319p^{55}+463956251p^{54}+425848438p^{53}+381586855p^{52}+333206745p^{51}+282279538p^{50}+230643333p^{49}+179888588p^{48}+131967562p^{47}+88501935p^{46}+49898964p^{45}+16982435p^{44}-9704613p^{43}-29913744p^{42}-44261457p^{41}-53507881p^{40}-57536634p^{39}-57915638p^{38}-55967523p^{37}-51361677p^{36}-45191378p^{35}-38803251p^{34}-32782977p^{33}-26686848p^{32}-20615057p^{31}-16216861p^{30}-12418840p^{29}-8579562p^{28}-6304843p^{27}-4764499p^{26}-3129542p^{25}-1863846p^{24}-1395239p^{23}-1462514p^{22}-869442p^{21}-527244p^{20}-943722p^{19}-776136p^{18}-492630p^{17}-578484p^{16}-599406p^{15}-433284p^{14}-197958p^{13}-273489p^{12}-303996p^{11}-90513p^{10}-74961p^{9}-128457p^{8}-89163p^{7}-40860p^{6}-25245p^{5}-42354p^{4}-23616p^{3}-1728p^{2}-6912p-4608,$

and its denominator is

$1152p^{29}(p+1)^4\left(p^2+p+1\right)^2\left(2p^5+2p^4+2p^2+p+2\right)^2\left(2p^5+2p^4+2p^3+p+2\right)\left(p^6+p^3+1\right)^2\left(p^8$

The numerator of the upper bound is

$18432p^{79}+129024p^{78}+460800p^{77}+1161216p^{76}+2386944p^{75}+4359168p^{74}+7379712p^{73}+11747328p^{72}+17748096p^{71}+25694592p^{70}+35852016p^{69}+48404832p^{68}+63449888p^{67}+80981856p^{66}+100835820p^{65}+122622272p^{64}+145866608p^{63}+169928324p^{62}+194113584p^{61}+217695724p^{60}+239614920p^{59}+258771236p^{58}+274527695p^{57}+286594374p^{56}+294417541p^{55}+297202091p^{54}+294919645p^{53}+287859977p^{52}+276580118p^{51}+261699133p^{50}+243585902p^{49}+222782260p^{48}+199966725p^{47}+176290792p^{46}+152830068p^{45}+129918421p^{44}+108087373p^{43}+87632330p^{42}+68892686p^{41}+52628009p^{40}+38962249p^{39}+27479808p^{38}+17856875p^{37}+10294777p^{36}+4909118p^{35}+1294165p^{34}-1193987p^{33}-2933860p^{32}-3686560p^{31}-3709051p^{30}-3511896p^{29}-2885964p^{28}-2259602p^{27}-2058252p^{26}-1636237p^{25}-946800p^{24}-622598p^{23}-708967p^{22}-604536p^{21}-297174p^{20}-391890p^{19}-501822p^{18}-263943p^{17}-246318p^{16}-480525p^{15}-438129p^{14}-117180p^{13}-114345p^{12}-334245p^{11}-195354p^{10}+25992p^{9}-29601p^{8}-144288p^{7}-69084p^{6}+42408p^{5}-34776p^{4}-64368p^{3}+8604p^{2}-1440p-14400,$ and its denominator is

$4608p^{29}(p+1)^4\left(p^2-p+1\right)\left(p^2+p+1\right)^2\left(2p^5+2p^4+2p^3+p+2\right)^2\left(p^6+1\right)\left(p^6+p^3+1\right)^2\left(p^{12}+p^{9}\right.$

The difference between the two bounds has order $p^{-9}$. We can then summarize

the results in the following:

**Theorem 9.1.1.** *Let $p$ be a prime greater than or equal to 31, then the probability of solubility over $\mathbb{Q}_p$ of a rational plane quartic is*

$$\rho(\mathbb{Q}_p) = 1 - \frac{1}{2}p^{-4} + \frac{1}{5}p^{-5} - \frac{9}{8}p^{-6} + \frac{41}{24}p^{-7} - \frac{35}{16}p^{-8} + O\left(p^{-9}\right).$$

Then we can compute the first 13 exact digits of $\rho(31)$, since the error is bounded by $10^{-31}$. Indeed, we have

$$\rho(31) \simeq 0.9999994923152.$$

If we evaluate the difference between the lower bound and upper bound at $p = 31$, where the error attains the greater value, we get $1.95110 \times 10^{-13}$.

The precision of the expression for $\rho(\mathbb{Q}_p)$ can be improved by computing sharper bounds for the solubilities of each reduction. In particular, the estimates on the probability of solubility of the double conic are the less accurate ones. If more precise bounds were achieved we would be able to get down to an error bounded by $p^{-11}$. Moving forward, the next bottle-neck would be the product of two double lines. In general, as discussed in the previous chapters, most of the troubles come from the non-reduced reductions.

In any case we can already estimate numerically quite precisely the value of $\rho(Q_p)$ by the fact that the error is bounded by $p^{-9}$. If we want an exact bound on the product of $\rho(Q_p)$ for $p \geq 31$ we can use the Riemann zeta function $\zeta(s)$. Indeed, we have $1 - p^{-4} < \rho(\mathbb{Q}_p) < 1 - p^{-5}$, for $p \geq 31$. Considering the product over the primes greater than or equal to 31, we obtain

$$\prod_{p=31}^{\infty} 1 - p^{-4} < \prod_{p=31}^{\infty} \rho(\mathbb{Q}_p) < \prod_{p=31}^{\infty} 1 - p^{-5}.$$

The first and the last terms can be expressed by the zeta function through the formula

$$\prod_{p} 1 - p^{-s} = \frac{1}{\zeta(s)}$$

and computing the first factor of the product for $p \leq 29$. In this way we conclude that

$$0.9999969802 < \prod_{p=31}^{\infty} \rho(\mathbb{Q}_p) < 0.9999999226.$$

We remark that numerically it is possible to achieve sharper bounds.

### 9.1.1 $\rho(\mathbb{Q}_p)$ for small primes

Now we give some estimate for the primes smaller than 31. For $p = 2$ most of the probabilities of solubility from the tables are still valid, the main uncertainty coming from the irreducible quartics. Among the 25536 irreducible plane quartics defined over $\mathbb{F}_2$, 24254 curves have at least one smooth point, which guarantees solubility. Between the 5082 curves that are either the union of two distinct $\mathbb{F}_p$-conics or the union of a cubic and a line, 5050 curves have a smooth point. Adding this information to the formulas of solubilities for the other cases gives us that at least 95.1403% of rational plane quartics are solvable over $\mathbb{Q}_2$. Looping through the irreducible quartics defined over $\mathbb{F}_3$, we obtain that $\rho(\mathbb{Q}_3) \geq 0.985417$. For the primes between 5 and 29 it is hard to describe a heuristic: the principal contribution to $\rho(\mathbb{Q}_p)$ is given by the smooth quartics. When $p \leq 29$ there exist pointless smooth quartics defined over $\mathbb{F}_p$; they have been counted by Bergström, Faber and van der Geer in the article [BCvdG14]. We warmly thank Everett W. Howe for his counts for the pointless smooth quartics that confirm the counts from [BCvdG14]. Here is the count:

| $p$ | Cardinality of smooth pointless curves |
|---|---|
| 2 | 165 |
| 3 | 29484 |
| 5 | 6277500 |
| 7 | 102056220 |
| 11 | 1364341550 |
| 13 | 2406275235 |
| 17 | 3909490272 |
| 19 | 4233511980 |
| 23 | 3721739296 |
| 29 | 5204490655 |

Notice that $\rho(\mathbb{Q}_p)$ is an increasing function tending to 1 with order 4, indeed $\rho(Q_p) \simeq 1 - p^{-4}/2$. Moreover, the upper bound for the probability of solubility is valid for any $p$. Now we can compute bounds for all the $\rho(\mathbb{Q}_p)$ for small primes:

Using all these bounds we can say that

| $p$ | $\leq \rho(\mathbb{Q}_p)$ | $\rho(\mathbb{Q}_p) \leq$ |
|---|---|---|
| 2 | 0.951403 | 0.986642 |
| 3 | 0.985417 | 0.992874 |
| 5 | 0.985417 | 0.998643 |
| 7 | 0.985417 | 0.999714 |
| 11 | 0.985417 | 0.999968 |
| 13 | 0.985417 | 0.999984 |
| 17 | 0.985417 | 0.999995 |
| 19 | 0.999997 | 0.999999 |
| 23 | 0.999998 | 0.999999 |
| 29 | 0.999999 | 0.999999 |

Table 9.4: Bounds for $\rho(\mathbb{Q}_p)$

**Theorem 9.1.2.** *The density $\rho$ of rational plane quartics that are everywhere local soluble satisfies*

$$84.93\% \leq \rho \leq 97.79\%.$$

Considering the Monte Carlo simulation for $\rho(\mathbb{R})$ and some evaluations on the value of $\rho(\mathbb{Q}_p)$ for $p \in 5, \ldots, 29$ we estimate $\rho \simeq 0.92$.

## 9.2 Semi-stable reductions

While computing the probabilities of solubility, we noticed that most of the difficult issues come from reductions that are not semi-stable. In section 3-C of the book by Harris and Morrison's book [HM06] is a description of how to obtain a semi-stable reduction from a non-semistable one, through blow ups and base changes. Based on that, a possible work-around would be to use this method in order to deal just with semi-stable reductions and then compute the overall probability of local solubility. A key problem of this process is describing the distribution of the curves when we act through those transformations. In the previous chapters we used linear change of coordinates, that are Haar measure-preserving. Whereas, when we blow up singularities of a family of curves it is hard to keep track of the density of such family through the procedure. In particular, we would need the density of the preimage of each semi-stable reduction in order to compute the probability of local solubility. Solving this issue would let us to compute $\rho(\mathbb{Q}_p)$. Indeed, in Chapter 7 we discussed all the semi-stable reductions, describing by

exact formulas each probability of solubility. This would lead us to compute an exact formula of the probability of local solubility for all the plane quartics.

# Bibliography


[AP95] Y. Aubry and M. Perret. A Weil theorem for singular curves. *Proceedings of Arithmetic,Geometry and Coding Theory IV*, 1995.

[BA] B.Büeler and A.Enge. Vinci. `https://www.math.u-bordeaux.fr/~aenge/?category=software&page=vinci`.

[Bal97] K. Ball. An elementary introduction to modern convex geometry. *Math. Sci. Res. Inst. Publ.*, 31, 1997.

[BCF] M. Bhargava, J. Cremona, and T. Fisher. The density of hyperelliptic curves over $\mathbb{Q}$ of genus $g$ that have points everywhere locally. *Unpublished draft preprint.*

[BCF15a] M. Bhargava, J. Cremona, and T. Fisher. The proportion of plane cubic curves over $\mathbb{Q}$ that everywhere locally have a point. *International Journal of Number Theory*, 12(4), 2015.

[BCF+15b] M. Bhargava, J. Cremona, T. Fisher, N. Jones, and J. Keating. What is the probability that a random integral quadratic form in $n$ variables has an integral zero? *International Mathematics Research Notices*, 2016(12):3828–3848, 2015.

[BCvdG14] J. Bergström, C.Faber, and G. van der Geer. Siegel modular forms of degree three and the cohomology of local systems. *Selecta Mathematica*, 20, 2014.

[Ber81] D. Bernardi. Hauteur $\mathfrak{p}$-adique sur les courbes elliptiques. *Seminar on Number Theory, Paris 1979–80*, 12:1–14, 1981.

[Ber05] D. J. Bernstein. Factoring into coprimes in essentially linear time. *Journal of Algorithms*, 54:1–30, 2005.

[Ber08] J. Bergström. Cohomology of moduli spaces of curves of genus three via point counts. *Journal für die reine und angewandte Mathematik*, 622:155–187, 2008.

[Bha14] M. Bhargava. A positive proportion of plane cubics fail the hasse principle. *arXiv preprint*, 02 2014.

[Ble04] G. Blekherman. Convexity properties of the cone of nonnegative polynomials. *Discrete and Computational Geometry*, 32(3), 2004.

[BM] J. Bost and J. Mestre. Computation of archimedean height of points of elliptic curves by quadratically convergent algorithm and application to the computation of the capacity of the union of two intervals. *Unpublished notes.*

[Bra10] R. W. Bradshaw. Provable computation of motivic l-functions. *PhD thesis*, 2010.

[Bru06] N. Bruin. *Some ternary Diophantine equations of signature (n, n, 2)*, pages 63–91. Springer Berlin Heidelberg, 2006.

[BS14] B. Barak and D. Steurer. Sum-of-squares proofs and the quest toward optimal algorithms. *proceedings of ICM 2014*, 2014.

[Coh00] H. Cohen. *Advanced Topics in Computational Number Theory.* Springer, 2000.

[CPS06] J. E. Cremona, M. Prickett, and S. Siksek. Height difference bounds for elliptics curves over number fields. *Journal of Number Theory*, 116:42–68, 2006.

[CT13] J. E. Cremona and T. Thongjunthug. The complex AGM, periods of elliptic curves over $\mathbb{C}$ and complex elliptic logarithms. *Journal of Number Theory*, 133(8):2813–2841, 2013.

[DL01] J. Denef and F. Loeser. Definable sets, motives and $p$-adic integrals. *Journal of the American Mathematical Society*, 14(2):429–469, 2001.

[Dup06] R. Dupont. *Moyenne Arithmetico-Géométrique, suites de Borchard et applications.* PhD thesis, Ecole Polytechnique, 2006.

[Har77] Robin Hartshorne. *Algebraic geometry.* New York, 1977. Graduate Texts in Mathematics, No. 52.

[Hil88] D. Hilbert. Über die darstellung definiter formen als summe von formenquadraten. *Math. Ann.*, 32:342–350, 1888.

[HLT05] W. E. Howe, K. Lauter, and J. Top. Pointless curves of genus three and four. *Algebra, Geometry, and Coding Theory (AGCT 2003)*, pages 125–141, 2005.

[HM06] J. Harris and I. Morrison. *Moduli of curves*, volume 187. Springer Science & Business Media, 2006.

[KS99] N. M. Katz and P. Sarnak. Random matrices, frobenius eigenvalues, and monodromy. *American Mathematical Society Colloquium Publications*, 45, 1999.

[LRRJ18] R. Lercier, C. Ritzenthaler, F. Rovetta, and J.Sijsling. Spanning the moduli space of curves and applications to smooth plane quartics over finite fields. *arXiv preprint*, 2018.

[Mot67] T. S. Motzkin. The arithmetic-geometric inequality. *Inequalities (Proc. Sympos. Wright-Patterson Air Force Base, Ohio, 1965)*, page 205–224, 1967.

[MS16] J. S. Müller and M. Stoll. Computing canonical heights on elliptic curves in quasi-linear time. *LMS Journal of Computation and Mathematics*, 19(A):391–405, 2016.

[Nie12] J. Nie. Discriminants and nonnegative polynomials. *Journal of Symbolic Computation*, 47(2):167 – 191, 2012.

[PAV+] A. Papachristodoulou, J. Anderson, G. Valmorbida, S. Prajna, P. Seiler, and P. A. Parrilo. SOSTOOLS: Sum of squares optimization toolbox for MATLAB. `http://www.eng.ox.ac.uk/control/sostools`.

[PV04] B. Poonen and J. Voloch. Random diophantine equations. *Progress in Mathematics - Boston*, 226:175–184, 2004.

[PW98] V. Powers and T. Wörmann. An algorithm for sums of squares of real polynomials. *Journal of Pure and Applied Algebra*, 127(1):99 – 104, 1998.

[Sag18] Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.2)*, 2018. `http://www.sagemath.org`.

[Sei54] A. Seidenberg. A new decision method for elementary algebra. *Annals of Mathematics*, 60(2):365–374, 1954.

[Sel51] E. S. Selmer. The diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Mathematica*, 85:203–362, 1951.

[Sil88] J. H. Silverman. Computing heights on elliptic curves. *Mathematics of Computation*, 51(183):339–358, 1988.

[Sil99] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, 1999.

[Sil08] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, 2008.

[Stö93] K.O. Stöhr. On poles of regular differentials of singular curves. *Bulletin of the Brazilian Mathematical Society*, 24:105–136, 1993.

[Was08] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Chapman & Hall/CRC, 2008. Second Edition.

[Zag87] D. B. Zagier. Large integral points on curves. *Mathematics of Computation*, 48:425–436, 1987.

[ZG98] W. A. Zúñiga-Galindo. Number of rational points of a singular curve. *Proceedings of the American Mathematical Society*, 126(9):2549–2556, 1998.